Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Colin J. Bennett
Associate Professor
Department of Political Science
University of Victoria
Victoria, B.C. V8W 3P5
CANADA

Paper prepared for Industry Canada, May 1996

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
  - The Receipt, Verification and Approval of Privacy Codes
  - The Receipt, Investigation and Resolution of Complaints

- Audit Powers
- Enforcement Powers
- Advice on the Privacy Implications of New Technologies
- Public Education and Research
- Sanctions and Remedies

- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendix 1
- Appendix 2
- Appendix 3
- Appendix 4
- Appendix 5

Task Force Home Page

Help What's New Sitemap Feedback About Us Français Top of Page

Canada

Last modified - 10/04/2000

Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendices

INTRODUCTION

On March 25th, 1996 Industry Canada hosted a workshop on Exploring the Oversight Function for Personal Data Protection in the Marketplace. In the morning session representatives from the Netherlands, New Zealand, Quebec, Hong Kong and the United States explained how data protection law is

administered and enforced in their respective societies. In the afternoon, the participants engaged in a roundtable discussion on the implementation of data protection policy in the Canadian context. The Canadian representatives included officials from federal government departments, the Office of the Privacy Commissioner (OPC), the provincial Information and Privacy Commissioner and Ombudsman offices, and the Canadian Standards Association (CSA).

I was asked by Industry Canada to be the rapporteur for this workshop and to write a report on the day's events. The views expressed in this paper, however, are not a strict report of all that was said at the workshop and no views are attributed to any of the participants. Rather the paper is a set of personal reflections on the various options for extending privacy protection rules to the private sector in the light of the very informative discussion on this occasion. These views are mine and mine alone, even though they have been shaped by numerous conversations with experts and officials both before and after the March 25th workshop.

The paper also builds upon my own previous work on the implementation of privacy protection policy in other countries, especially Regulating Privacy: Data Protection and Public Policy in Europe and the United States, and upon the research conducted on the implementation of the Canadian Standards Association's Model Code for the Protection of Personal Information (Q830). The paper also draws upon other comparative and Canadian analysis of the implementation of privacy protection policy. In particular, the 1995 report by Ian Lawson set out a complete range of regulatory options for the protection of privacy on the information highway. This paper attempts to narrow the focus, and to concentrate on the most practical regulatory options for Canada.

Although there is plenty of scope to draw lessons from Canadian and overseas experience, we are not working with a tabula rasa. There are public sector laws at the federal level, and in most provinces. In Quebec's Bill 68, we have the only legislation in Canada that regulates private sector practices. Each of these statutes grants a different range of powers and responsibilities to the respective offices of Information and Privacy Commissioners (see Appendices). In addition, there are a plethora of other provisions within provincial and federal statutes that relate to the collection, storage, processing and transmission of personal data. Many businesses have also developed voluntary "codes of practice." It is impossible to "wipe the slate clean" and to build a privacy protection regime from the ground up. The policy process will be inescapably incremental. It must build upon the instruments and provisions that are already in place.

The paper will also not grapple with the complicated issue of federal/provincial constitutional authority. To a large extent, questions about the appropriate oversight and compliance mechanisms will apply whether or not legislation is crafted with a comprehensive scope, or whether it applies more narrowly to federally regulated entities. This paper addresses the functions that need to be performed in any effective regime for personal data protection. Those functions will require careful analysis whether they are performed at the federal and/or provincial levels, or on a comprehensive or sectoral basis. This paper is about the level of regulation. Jurisdictional conflicts will continue to occur under any legislated or self-regulatory scheme.

I am, therefore, indebted to those people who attended the March 25th workshop. This paper cannot purport to offer any consensus on the results of

that meeting. Nevertheless, I hope that those present recognize from this paper the most important themes and issues discussed on that occasion. I am also grateful to Ritu Mahil for her research assistance.

Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendices

THE NATIONAL STANDARD FOR PRIVACY PROTECTION

In its 1995 report the Information Highway Advisory Council (IHAC) advised the federal government to:
create a level playing field for the protection of personal information on the Information Highway by developing and implementing a flexible legislative

framework for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA model code, while allowing the flexibility to determine how they will refine their own codes.

The report goes on to recommend that the federal government "in cooperation with the CSA Working Group on Privacy and other interested parties, study the development of effective oversight and enforcement mechanisms." This paper is a contribution to that effort.

On May 23, Industry Minister Manley released the government's response to the IHAC report in which it was concluded that "the right to privacy must be recognized in law, especially in an electronic world of private databases where it is all too easy to collect and exploit information about individual citizens." Hence:
As a means of encouraging business and consumer confidence in the Information Highway, the Ministers of Industry and Justice, after consultation with the provinces and other stakeholders, will bring forward proposals for a legislative framework governing the protection of personal data in the private sector.

The government's response explicitly mentions the Model Code for the Protection of Personal Information from the Canadian Standards Association as a legislative framework. The following principles have been widely agreed by representatives from government, industry and consumer associations. They represent an important consensus on the basic principles of a privacy protection policy:

- *Accountability*
An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

- *Identifying Purposes*
The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected

- *Consent*
The knowledge and consent of the individual are required for the use, or disclosure of personal information, except where inappropriate.

- *Limiting Collection*
The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

- *Limiting Use, Disclosure and Retention*
Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

- *Accuracy*
Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

- *Safeguards*

Personal Information shall be protected by security safeguards appropriate to the sensitivity of the information.

- *Openness*

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

- *Individual Access*

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

- *Challenging Compliance*

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

The goal of any national privacy protection policy should be to implement these principles throughout all organizations that process personal data (in both public and private sectors).

This goal requires voluntary action from the "bottom-up" as well as regulatory action from the top-down. There are a range of tools within the repertoire of possible policy instruments. Four are outlined within Industry Canada's 1994 publication Privacy and the Canadian Information Highway: legislation and regulation; voluntary codes and standards; technological solutions; and consumer education. Although this paper concentrates on the relationship between law, regulation, codes and standards, it should never be forgotten that technologies of privacy (such as public-key encryption) have a crucial role to play in any privacy policy. Moreover, no policy can succeed without the actions of an informed and vigilant citizenry. Each of these four approaches contributes to a "mosaic of solutions." Each is a necessary condition for privacy protection on the information highway; none is a sufficient condition.

Task Force Home Page

Help What's New Sitemap Feedback About Us Français Top of Page

Canada

Last modified - 10/04/2000

Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendices

THE VALUE OF THE PRIVACY STANDARD

The status quo has been described as a "privacy patchwork." A comprehensive data protection law covering all private sector organizations in Quebec contrasts with a hodgepodge of voluntary codes and isolated statutory provisions in the rest of the country. Partly as a response to this

incoherence, the Canadian Standards Association (CSA) has recently developed a Code for the Protection of Personal Information in association with stakeholders from government, consumer groups and key industry sectors (banking, telecommunications, insurance, direct-marketing, credit-reporting). This Code was ratified without any dissent in September 1995 and was released in March 1996. It was designed to add some uniformity to data protection policy and practice within the Canadian private sector.

At first glance, the CSA Model Code might seem a Canadian version of the OECD Guidelines -- a rearrangement and translation of the key principles into the Canadian context. At the moment, it is just that -- a model that any organization can use and adapt to their specific circumstances. But it does represent a very important consensus, brokered among the major stakeholders. Moreover, it has doubtless been very valuable for participants in the process to think about the privacy protection problem from scratch and to grapple with these complex issues.

Although no decision has yet been made about the mechanisms for implementation and oversight, the CSA Model Code is a "standard" that might be subjected to the same kind of certification and registration procedures that are used for other standards. Privacy, of course, is not the kind of "hard" standard typically used within manufacturing industry. Nevertheless it does have certain parallels with the range of "quality management standards" within the ISO-9000 series that have been rapidly permeating the Canadian and American private sectors, as well as with environmental standards in the ISO 14000 series. Thus, in the same way that a company might be forced to register to ISO-9000 to convince its clients and customers that it has adopted a level of "quality assurance" the same system of accreditation could be developed to the privacy standard, where effective data protection is demanded within the Canadian or international marketplace. The price of maintaining a registration to the standard would be an agreement to have independent and regular privacy audits.

Of course, not all businesses would be expected to go to the kind of trouble and expense of registering to ISO-9000. The registration scheme for privacy would also require procedures applicable to the smaller business. The scheme requires an appropriate balance between the encouragement of registration on the one hand, and the prevention of symbolic claims about policies and practices on the other. It also requires an appropriate publicity vehicle, so that any consumer can find out who has registered to the standard and who has not. A "Privacy Good Book" in the form of a Privacy Register would have to accompany the registration scheme.

If a credible registration process is established, the CSA Model Code ceases to be a "voluntary" mechanism. Organizations would have to produce a code and a related set of operational guidelines and be subjected to regular and independent auditing of their practices. The system would build a more consistent and credible system of verification than occurs at the moment. It could satisfy international and contractual requirements. It could provide a more common and consistent yardstick by which to observe and evaluate company practices. Such a system would be able to monitor the claims made by organizations about their policies and practices.

I have suggested that the privacy standard might filter throughout the marketplace by a number of different inducements to registration: by moral suasion; by the desire to avoid adverse publicity; by the desire to gain a competitive advantage; by the reference to the standard in private contract;

by the registration to the privacy standard in conjunction with registration to ISO-9000; by the reference to the standard when government "contracts out" data processing services; by pressure from research-funding agencies; by the regulation of interprovincial data flows in Quebec's Bill 68; and by the use of the "adequacy" provisions by European data protection authorities. Canadian and foreign regulatory bodies can insist that the receipt of personal data within Canada be accompanied by a registration to the CSA Model Code.

As outlined, the registration to the CSA Model Code would provide a better yardstick for the evaluation of personal information practices. It could promote higher levels of consumer awareness. It could raise the levels of responsibility and accountability within Canadian business. It can initiate more and better privacy auditing. But the process would still be incremental and piecemeal. It could never achieve the kind of uniform legal standard in Canada, the "seamless protection" that the Federal Privacy Commissioner has called for.

Task Force Home Page

Help What's New Sitemap Feedback About Us Français Top of Page

Canada

Last modified - 10/04/2000

Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendices

THE VALUE-ADDED OF DATA PROTECTION LAW

Leaving aside the peculiar constitutional dilemmas within Canada, what would a legal regime add to the standards-approach monitored through a registration regime administered through an accredited standards-registration body? Five arguments are persuasive.

First, only law can express the standards of the community, the line beyond which no organization should be allowed to cross. This is what Bruce Phillips has in mind when he argues that "unless some sensible rules of traffic management are a part of these systems, the first roadkill will be our personal privacy and dignity." The metaphor of the "information highway" does lead naturally to the undeniable argument that there needs to be some consistent "rules of the road." For many businesses the rules of the road might be attractive to create a "level-playing field" – a clear and consistent set of privacy rules that apply across the entire Canadian marketplace.

Law does not necessarily provide that standard. "Far too frequently," Oscar Gandy reminds us, "we tend to talk about the law as the even-handed instrumentality that ensures that the universal values claimed for any society are protected and guaranteed." Any advocate for a legal regime must recognize the vast inequalities within the operation of the law, especially when it is used as a "strategic weapon" rather than as "an expression of a basic moral vision, a set of guiding principles that serve as foundations supporting relations among persons."

Second, those "rules of the road" are more likely to be even-handedly applied under the guidance of an impartial "traffic cop." The CSA Model Code states that each organization shall designate an individual who is responsible for compliance, and that organizations shall make it clear how consumers might challenge compliance with the principles (Principles One and Ten). Under current circumstances, the highest mechanism for complaint resolution within most sectors is within the business that is processing the personal data. Only legislation can establish a final arbiter external to the organization. Only legislation can involve the institutions that to date have the best experience with resolving privacy complaints within Canada -- the offices of the federal and provincial Information and Privacy Commissioners.

Third, only law can bring the recalcitrants into line. However successfully the CSA Model Code can regulate the practices of the most responsible businesses, there will always be a minority that will see a competitive advantage in processing personal data in contravention of the standard. Undoubtedly, the fear of the CDMA that the image of its responsible members is being tarnished by a minority of non-members motivated its call for national legislation based on the CSA standard. This move is fascinating. It indicates that at a certain point for some sectors, legislation becomes the acceptable alternative to continued bad publicity.

Fourth, an economic argument can be advanced. As Ian Lawson has argued: "To the extent that business obtains and uses personal information without a market mechanism to govern the exchange, business is a classic free rider in the economy. It consumes a common property resource without covering the externalities related to its extraction and use." So when organizations benefit from the use of the information, either themselves or by trading that information to third parties, no benefits accrue to the original information provider. That situation has perpetuated because of the reluctance of many businesses to be transparent about their practices and to establish mechanisms to obtain informed consent when they wish to use personal information for "secondary uses." Business remains a "free rider" so long as individuals are kept in the dark about how their information is being used and disclosed.

Classic economic theorizing would contend that an imperfect marketplace can be rectified by two mechanisms. First, one can give a value to personal

information so that the costs and benefits of transactions are allocated more appropriately. There have been some proposals for market-based solutions to this imbalance; all rest on schemes to give individuals some property rights over their information with appropriate compensation when it is used for purposes other than those for which it was originally supplied. The other solution is regulatory intervention to redress the marketplace imbalance. It is contestable, of course, that economic theorizing has any role to play in the protection of a fundamental human right. Nevertheless, even according to the principles of neoclassical economic reasoning, the arguments for regulatory intervention are hard to resist.

Fifth, only the law can harmonize the standards of the public and the private sectors. Where the "public" sector ends and the "private" sector begins is increasingly difficult to determine. Questions raised about the application and meaning of the privacy provisions in the Federal Privacy Act and related provincial statutes will have an evolving impact on the practices of the private sector. It can also be expected that the increased publicity that privacy issues will receive in the media as a result of the efforts of the Privacy Commissioners will continue to have some spill-over effect. The need for "seamless protection" between the private and public sectors was one key factor behind the passage of the New Zealand Privacy Act.

The distinction is also being eroded by efforts to privatize or hive-off government functions. Thus "private" organizations are increasingly performing "public" functions, and often require the use of "public" data to fulfill those obligations. Illustrations include: the use of smart cards and ATM machines for the dispensing of government benefits; the matching of data on welfare recipients with bank or financial records to ascertain eligibility; the trading of government personal information to enhance revenue; the use of credit reports for security checks, and so on. The pervasiveness and flexibility of the new technologies will make it increasingly difficult to determine which data are "in" the public sector, and which "in" the private.

Finally, and the least important reason, concerns the interpretation of Article 25 of the new European Directive on data protection:

The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

Notwithstanding the stipulation in Article 26 that "professional rules and security measures which are complied with" may be taken into account in determining the "adequacy of protection," Article 25 could mean that European regulators might legitimately interrupt flows of data to every part of Canada except Quebec, unless legal protections are forthcoming. An "adequate level of protection" could be interpreted to mean a legislated regime, overseen by an independent "supervisory authority." At the very least, it should be noted that any professional rules (such as codes of practice) have to be complied with. Any data protection system in Canada has to demonstrate that it is seriously and effectively implemented.

Task Force Home Page

Help What's New Sitemap Feedback About Us Français Top of Page

Canada

Last modified - 10/04/2000

Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendices

LEGISLATING TO THE STANDARD

Unlike voluntary codes of practice, the CSA standard can be referenced in law. Around one-third of CSA's published standards have been referenced either in federal and/or provincial legislation. Most of these standards relate to the technical standards for products procured by government. Increasingly,

however, performance standards, such as those for quality management or environmental protection, are being used in order to implement statute, regulation and court-order. There is nothing to stop federal and/or provincial authorities using Q830 in a similar way.

The report of the Information Highway Advisory Council, however, envisages a more comprehensive approach -- a "flexible legislative framework for both public and private sectors. Legislation would require sectors or organizations to meet the standard of the CSA model code, while allowing the flexibility to determine how they will refine their own codes." This seems to contemplate "framework" or "shell" legislation at the federal level; a statement of principles and obligations, leaving the functions of complaints resolution, investigation, auditing, and so on, as a matter for further analysis "in cooperation with the CSA Working Group on Privacy." But there have been a number of different interpretations of what IHAC means and of what it means to "legislate to the standard."

The Canadian Direct Marketing Association, for example, called upon Minister Manley:
to place before Parliament framework federal legislation that requires each industry sector to develop its own specific privacy code that meets a national standard. We do not think this legislation needs to be complex, nor would it be expensive to administer. We suggest a similar model to that of the Canada Health Act that sets minimum national standards but allows each province to develop and run its own health care system to meet its specific needs.

The CDMA goes on to explain that "each code would reflect the needs of the individual sector and meet the standards set by the OECD and/or draft CSA codes." Moreover, the CDMA also has "concerns that regulatory authority could be used to make the principles more onerous. We think the concept of allowing industries to create standards that protect privacy and meet their particular needs will prevent undue regulatory interference." The CDMA would delegate a small complaints-resolution function to the Federal Privacy Commissioner.

There is a key distinction between voluntarism and self-regulation. The former implies that public policy should remain indifferent to the policies and practices pursued. It implies that government should simply trust business to pursue privacy-friendly practices but has no interest in setting an overall standard. This has been the position of the Canadian and American federal governments to date. A self-regulatory regime, on the other hand, establishes in law the standard and grants business the authority to regulate its own practices. The key difference is that a legislated standard is set, and that both individual and organization knows that when self-regulation breaks down, the policy instruments established under the law can intervene.

The Federal Privacy Commissioner has a slightly different vision, suggesting that the CSA Model Code could form an amendment to the Privacy Act. This option is attractive to the Privacy Commissioner as it would "embody in law a set of rules devised by a committee representing a broad cross-section of Canadian private enterprise." However, the Privacy Commissioner says nothing about "codes." For him the advantage of legislating to the standard is that "observance of the CSA standards would become a legal obligation and would be supported by a system of independent oversight."

Ian Lawson also recognizes the "unique consensus that is emerging between government, consumers and industry players" and that is reflected in the CSA

Model Code. For him, the "higher purpose of the Model Code is for it to be adopted-by-reference as a legislative standard to which the private sector must comply as a condition of using personal information on the information highway."

Lawson outlines three possible options for federal regulation based on standards-enforcement. Under his "Light Version", framework legislation is enacted by the federal government with the operating provision that data users must comply with the CSA Model Code by developing an appropriate code that meets the industry standard. The model would rely entirely on the CSA as the monitoring instrument, and embodies no obvious role (beyond moral suasion) for the Privacy Commissioners.

Under his "Medium Version", the Privacy Commissioners would be "mandated to receive complaints from consumers relating to the data user's compliance with its code." The Commissioners apply "existing problem-solving techniques, including education, persuasion, and mediation." This then adds a layer of oversight to the CSA Model Code, in addition to any code verification and registration process established through an accredited registrar. It perhaps adds a more coherent and focussed method of redress for the aggrieved individual, and locates overall oversight responsibility within the institutions that have sole responsibility for, and expertise in, the privacy issue.

Under Lawson's "Heavy Version", the Privacy Commissioners would not only resolve complaints but would be "empowered to issue orders requiring data users to comply with their codes; disobedience of such orders is a criminal offence." The legislation would also establish civil liability for failure of a data user to comply with its code." Only under Lawson's "Heavy Version" would registration be underpinned by a set of legally enforceable rights, and be subjected to the general oversight of the Privacy Commissioners. Only under this version would a system of data protection be constructed that brings the full range of compliance mechanisms to bear on the problem.

The remainder of this paper builds upon Lawson's analysis and addresses in more detail the oversight functions under a system in which the CSA Model Code is referenced in federal and/or provincial legislation. If the law says that any business operating in Canada must comply with the CSA Model Code as a condition for using personal information on the information highway, what further responsibilities and obligations need to be assigned?

Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendices

THE OVERSIGHT FUNCTIONS

A functional approach to policy analysis begins with a statement of the functions that might be performed within any public policy, and only then considers the public and private agencies that might perform them. The discussion at that workshop on March 25th was organized according to the

following functions: the receipt, verification and approval of privacy codes; the receipt, investigation and resolution of complaints; enforcement powers; the auditing of organizations; advice on the privacy implications of new technology practices; education and research; and remedies and sanctions. This analysis is organized according to the same framework.

- The Receipt, Verification and Approval of Privacy Codes
- The Receipt, Investigation and Resolution of Complaints
- Audit Powers
- Enforcement Powers
- Advice on the Privacy Implications of New Technologies
- Public Education and Research
- Sanctions and Remedies

Task Force Home Page

Help What's New Sitemap Feedback About Us Français Top of Page

Canada

Last modified - 10/04/2000

Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendices

SUMMARY: THE ELEMENTS OF AN OVERSIGHT SYSTEM IN CANADA

It is now necessary to summarise the analysis to reach some tentative conclusions about the possible elements of an oversight system for the protection of personal information within Canada's private sector:

- Provincial and federal governments need to apply the full range of available policy instruments to the privacy problem: Self-regulatory codes, legislation, privacy-protecting technologies, and better programs for consumer education. These are the policy instruments. They are not mutually exclusive. They all need to be utilized.

- The three years of bargaining over the CSA standard represents a crucial stage in the policy-making process. The brokering of a consensus has been completed. Any legislated scheme needs to be based on this established accommodation.

- A private sector privacy protection law does not need to be burdensome or overly complicated. Canada should avoid the costly and bureaucratic licensing and registration systems that have been established in some European societies.

- On the other hand, law without an effective mechanism for compliance monitoring can be worse than no law at all, and would not be considered "adequate" to meet European standards.

- The central oversight agencies should be federal and provincial information and privacy commissioners (where they exist). These offices have established an independence, credibility and expertise. They are uniquely located within the regulatory landscape to oversee private sector legislation, and resolve issues that span the public/private divide.

- Any legislated scheme needs to establish a balance of responsibilities for the following functions: complaints resolution and mediation; complaints investigation; audits; advice on the privacy implications of new technologies; the promotion of codes of practice; public education; and research. The most effective remedies may be those that are general in nature and pro-active rather than reactive.

- Dispute resolution should be as non-litigious as possible, and should only be provided after all other avenues have been exhausted. Business will want quick and predictable resolution of privacy problems . There may be a persuasive case for a specialized federal/provincial Privacy Tribunal to resolve disputes over private sector issues.

- Registration to the CSA Model Code contributes a crucial mechanism for enforcement within any potential regulatory system . Registration to the privacy standard can complement almost any current or future, contractual or regulatory, provincial or federal, sectoral or comprehensive, provisions for personal data protection. It can be used to reward good practice, and to bring the recalcitrants into line.

- Privacy codes will obviously continue to play an important role within any legislated regime. The standards-registration process can relieve regulatory bodies of checking and verifying privacy code content. A system that mandates all organizations to develop privacy codes would be unnecessarily burdensome and expensive. Consequently, codes should continue to be developed as a result of market demand and consumer pressure but, only in special circumstances, in response to regulatory fiat.

- Overseas experience suggests that codes of practice that enjoy any form of legal status (beyond the evidentiary value) are difficult and time-consuming to negotiate. Privacy codes should be encouraged and they should use the CSA standard as a template. But under a legislated regime, they should not be given an official "seal of approval", nor the power to qualify the provisions of the law. However, compliance with a code approved by CSA may be taken into account by Commissioners and courts in determining whether there has been a breach of the privacy principles.

- Experience suggests that sanctions in the form of fines are not a significant inducement toward compliance. Civil remedies are also ineffective because of the difficulty of proving actual damages from the willful mistreatment of personal data.

- In the context of private sector oversight, the threat of bad publicity can go a long way to securing compliance with the data protection principles. This incentive is probably a lot higher in the private, than in the public, sectors. The public reporting process is, therefore, crucial within any oversight model.

- It may be that the most effective sanction is a regulatory power to order registration to the standard. Thus if a pattern of complaints arose about a particular business, privacy commissioners or the courts could require registration to the standard, triggering the code development and audit process and passing the costs to the data user.

Task Force Home Page

Help What's New Sitemap Feedback About Us Français Top of Page

Canada

Last modified - 10/04/2000

Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendices

CONCLUSIONS: QUESTIONS FOR FURTHER ANALYSIS

These conclusions are not inconsistent with other recent policy analysis about data protection. They are, however, tentative and incomplete. I conclude with an inventory of some of the complex regulatory questions that still require careful analysis and debate.

The consistency of the CSA Model Code with existing Canadian and international privacy provisions?

If the principles within the CSA Model Code are to be given the force of law, there clearly needs to be careful analysis of the relationship between the wording of these principles and that within existing privacy legislation, including: the federal Privacy Act, the provincial Information and Privacy Acts, Quebec's Bill 68. In addition, we need analysis of its consistency with other private sector privacy provisions including those within the 1993 Telecommunications Act, the 1991 Bank Act, and the provincial consumer credit legislation. We also require careful comparison of the CSA Model Code with the EU Data Protection Directive.

What is the future relationship between the Privacy Commissioners and other federal and provincial regulators?

What should be the continuing role of federal regulators such as the Canadian Radio-Television and Telecommunications Commission (CRTC) and the Office of the Superintendent of Financial Institutions (OSFI)? The former in particular has been active in regulating uses of new technologies within the telecommunications sector. There is an argument that this regulatory power should not be diluted. At the provincial level, what would be the future role of regulators for insurance and consumer credit?

Should the privacy commissioners be empowered to restrict flows of personal data to societies that do not have adequate data protection?

One concern of the European data protection authorities is that personal data can flow through societies with "adequate" protection, to those without. Ideally each national data protection law would contain a transborder data flow restriction similar to that within Articles 2 5 and 26 of the EU Directive. If so, how should this power be exercised in Canada, and by whom? At what point do the fleeting and rapid electronic impulses that characterize international data flows become a matter for Canadian regulation?

Will compliance monitoring under the CSA standard be consistent with existing auditing schemes under the public sector legislation?

The Quality Management Institute of CSA is currently deciding on the most appropriate registration scheme to Q830. If registration to the standard is to be employed as a compliance monitoring process, we need a consistent audit guide, an accreditation scheme for privacy auditors, an appropriate publicity mechanism, a method to monitor claims made about business policies and practices, and possibly an appropriate symbol or cachet for the "privacy-friendly" business. Privacy commissioners need to have confidence in the registration process if the Model Code is to be employed in the same way as other quality management standards.

Can regulatory power be given in statute to require a registration to a standard?

This is an interesting innovation and a potentially very effective means of compliance monitoring. But what are the precedents for this power in other fields, such as government procurement, equity policy, environmental policy and so on? If subsequent violations occur within a business that is registered

to the standard, who shares the liability for any damages to the data subject?

What are the costs of an oversight regime, and by whom should they be borne? Are there opportunities for cost-recovery?

Oversight that is coordinated among the existing commissioners, systemic rather than specific, anticipatory rather than reactive, and educational rather than regulatory, is also likely to be more cost-effective. The use of the standards-registration process can also relieve Commissioners and other regulators of much compliance work, and pass the costs onto the data user.

What process should be used for federal/provincial coordination?

The federal/provincial constitutional question underpins this entire analysis. Little is possible without a cooperative arrangement between the federal and provincial governments on the appropriate legislative process. Lawson outlined six models, in addition to the "paramount national standards model": mirror legislation; jurisdictional abstention; contract; conditional legislation; concurrent legislation; collaborative/complementary model. To the extent that that process can be agreed, the resolution of these oversight and enforcement issues will be facilitated.

In conclusion, it can be noted that not everything needs to be firmly concluded and nailed down. Legislation is a framework; it needs to be adaptable to changing circumstances. It also needs to be accessible and user-friendly. The more complicated the legislative provisions, the less likely will the law be used as an instrument by ordinary citizens. From this discussion, however, may be emerging a distinctively Canadian approach to personal data protection. This approach emphasizes the use of all instruments within the "toolkit" of privacy protection. It recognizes that voluntary action from the "bottom-up", is just as necessary as regulatory action from the "top-down." And it comprises an innovative combination of the traditional ombudsman approach with the use of the relatively new instruments from the world of standards-setting and certification.

Task Force Home Page

Help What's New Sitemap Feedback About Us Français Top of Page

Canada

Last modified - 10/04/2000

Building Trust in the Digital Economy

- Security & Cryptography
- Authentication
- Privacy
  - Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector
- Consumer Protection

Privacy: The protection of personal information

Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector

Table of Contents

- Introduction
- 1. The National Standard for Privacy Protection
- 2. The Value of the Privacy Standard
- 3. The Value-Added of Data Protection Law
- 4. Legislating to the Standard
- 5. The Oversight Functions
- 6. Summary: The Elements of an Oversight System in Canada
- Conclusion: Questions for Further Analysis
- Appendices

APPENDIX 1 - Powers granted to Information and Privacy Commissioners in Complaints Investigation and Resolution

Federal

The Privacy Commissioner has the power:

- to summon and enforce the appearance of persons before the Privacy Commissioner and compel them to give oral or written evidence on oath and to produce such documents and things as the Commissioner deems requisite to the full investigation and consideration of the complaint, in the same manner and to the same extent as a superior court of record;

- to administer oaths;

- to receive and accept such evidence and other information...whether or not such evidence or information is or would be admissible in a court of law;

- to enter any premises occupied by any government institution on satisfying any security requirements of the institution relating to the premises;

- to converse in private with any person in any premises entered..and carry out inquiries within the authority of he Privacy Commissioner;

- to examine or obtain copies or extracts from books or other records found in any premises entered...containing any matter relevant to the investigation.

Ontario

- The commissioner may require to be produced and may examine any record that is in the custody or under the control of an institution, despite Parts II and III of The Freedom of Information and Protection of Privacy Act, 1987 and any other Act or privilege, and may enter and inspect any premises occupied by an institution for the purposes of the investigation.

- A head of an institution may require that the examination of record by the commissioner be of the original at its site.

- The commissioner may summon and examine on oath any person who, in the commissioner's opinion, may have information relating to the inquiry, and for that purpose the commissioner may administer oath.

B.C.

- In conducting an investigation the commissioner has the powers given to a commissioner by sections 15 and 16 of the Inquiry Act.

- The commissioner may require any record to be produced to the commissioner and may examine any information in a record, including personal information.

- Despite any other enactment or any privilege of the law of evidence, a public body must produce to the commissioner within 10 days any record or a copy of any record required.

- If a public body is required to produce a record...and it is not practicable to make a copy of the record, the head of that public body may require the commissioner to examine the original at its site.

Alberta

- In conducting an investigation...the commissioner has all of the powers, privileges and immunities of a commissioner under the Public Inquiries Act.

- The commissioner may require any record to be produced to the commissioner and may examine any information in a record, including personal information whether or not the record is subject to the provisions of the Freedom of Information and Protection of Privacy Act.

- Despite any other enactment or any privilege of the law of evidence, a public body must produce to the commissioner within 10 days any record or a copy of any record required.

- If a public body is required to produce a record...and it is not practicable to make a copy of the record, the head of that public body may require the commissioner to examine the original at its site.

Quebec (Public)

commission may investigate:

- a confidential file to determine if the nominative information contained therein was entered and used in accordance with the order; whether the confidentiality of personal information contained in a file held by a public body respecting the adoption of a person has been respected;

- whether the confidentiality of personal information contained in a file held by the Public Curator on a person whom he represents or of whose property he administers has been respected.

- The investigation is secret. Only a member of the commission of a member of its management staff designated in writing for that purpose by the commission may examine the nominative information entered in the file or the personal information contained in a file. However, a member of the staff of the commission may, if the commission so authorizes in writing, examine the personal information in a file.

Quebec (Private)

Any person authorized by the commission to make inquiries may:

- enter, at any reasonable time, the facilities of an enterprise carried on by a person collecting, holding, using or communicating personal information to third persons;

- examine and make copies of any personal information of whatever form.

- The commission may...inquire into or entrust a person with inquiring into any matter relating to the protection of personal information as well as into the practices of a person who carries on an enterprise and who collects, holds,

uses or communicates such information to third persons. APPENDIX 2

- Enforcement Powers of Information and Privacy Commissioners

APPENDIX 2 - Enforcement Powers of Information and Privacy Commissioners Federal

The Privacy Commissioner may:

- apply to the Court...for a review of any refusal to disclose personal information requested in respect of which an investigation has been carried out by the Privacy Commissioner, if the Commissioner has the consent of the individual who requested access to the information;

- appear before the Court on behalf of any individual who has applied for a review;

- with leave of the Court, appear as a party to any review applied for.

- The Court shall, if it determines that the head of the institution is not authorized under the Act to refuse to disclose the personal information, order the head of the institution to disclose the personal information, subject to such conditions as the Court deems appropriate, to the individual who requested access thereto, or shall make such other order as the Court deems appropriate.

Ontario

- After all of the evidence for an inquiry has been received, the Commissioner shall make an order disposing of the issues raised by the appeal.

- Where the Commissioner upholds a decision of a head that head may refuse to disclose a record or a part of a record, the Commissioner shall not order the head to disclose the record or part.

- The Commissioner's order may contain any terms and conditions the Commissioner considers appropriate.

B.C.

- If the inquiry is into a decision of the head of a public body to give or refuse to give access to all or part of a record, the commissioner must, by order, do one of the following:

- require the head to give the applicant access to all or part of the record, if the commissioner determines that the head is not authorized or required to refuse access;

- either confirm the decision of the head or require the head to reconsider it, it the commissioner determines that the head is authorized to refuse access;

- require the head to refuse access to all or part of the record, if the commissioner determines that the head is required to refuse access.

- If the inquiry is into any other matter, the commissioner may, by order, do one or more of the following:

- require that a duty imposed by this Act or the regulations be performed;

- confirm or reduce the extension of a time limit under section 10 of the Act;

- confirm; excuse or reduce a fee, or order a refund, in the appropriate circumstances, including if a time limit is not met;

- confirm a decision not to correct personal information or specify how personal information is to be corrected;

- require a public body to stop collecting, using or disclosing personal information in contravention of the Act;

- require the head of a public body to destroy personal information collected in contravention of the Act.

Alberta

- If the inquiry relates to a decision to give or to refuse to give access to all or part of a record, the Commissioner may, by order, do the following:

- require the head to give the applicant access to all or part of the record, if the Commissioner determines that the head is not authorized or required to refuse access;

- either confirm the decision of the head or require the head to reconsider it, if the Commissioner determines that the head is authorized to refuse access;

- require the head to refuse access to all or part of the record, if the Commissioner determines that the head is required to refuse access.

- If the inquiry relates to any other matter, the Commissioner may, by order, do one or more the following:

- require that a duty imposed by the Act or the regulations be performed; confirm or reduce the extension of a time limit under section 13 of the Act;

- confirm or reduce a fee or order a refund, in the appropriate circumstances, including if a time limit is not met;

- confirm a decision not to correct personal information or specify how personal information is to be corrected;

- require a public body to stop collecting, using or disclosing personal information in violation of the Act;

- require the head of a public body to destroy personal information collected in violation of the Act.

Quebec (Public)

- The Commission may, after investigating a personal information file or a confidential file and after giving the public body responsible for the file an opportunity to submit written observations:

- order that nominative information be corrected or deleted from the file or that the use of the file made contrary to the Act, the order or the prescriptions of the Commission, as the case may be, be discontinued;

- order the public body to take the measures it considers appropriate to meet the conditions provided for by this Act or the prescriptions of the Commission;

- order the destruction of a personal information file established or used contrary to the Act;

- recommend to the Government that the order authorizing the establishment of a confidential file be amended or revoked.

- On completion of an investigation...the Commission may:

- order the public body to take the necessary measures to ensure the confidentiality of the personal information contained in such a file respecting the adoption of a person;

- indicate the measures that must be taken to ensure the confidentiality of the personal information contained in such a file;

- indicate the special conditions to which the maintenance of such a file may be subject.

Quebec (Private)

- The Commission has all the powers necessary for the exercise of its jurisdiction; it may make any order it considers appropriate to protect the rights of the parties and rule on any issue of fact or law.

- The Commission may...order a person carrying on an enterprise to communicate or rectify personal information or refrain from doing so.

- A decision by the Commission becomes executory as a judgment of the Superior Court and has all the effects of such a judgment from the date of its homologation by the Superior Court.

• Following an inquiry relating to the collection, retention or communication of personal information by a person carrying on an enterprise, the Commission may, after giving the person an opportunity to present his observations, recommend or order the application of such remedial measures as are appropriate to ensure the protection of the personal information.APPENDIX 3 Advisory Functions of Information and Privacy Commissioners/Commissions on Privacy Implications of Legislation and Technologies

APPENDIX 3 - Advisory Functions of Information and Privacy Commissioners/Commissions on Privacy Implications of Legislation and Technologies

Federal

• The Privacy Commissioner may, at any time, make a special report to Parliament referring to and commenting on any matter within the scope of the powers, duties, and functions of the Commissioner.

Ontario

• The Commissioner may offer comment on the privacy protection implications of proposed legislative schemes or government programs.

B.C.

• The commissioner may:

• comment on the implications for access to information or for protection of privacy of proposed legislative schemes or programs of public bodies;

• comment on the implications for access to information or for protection of privacy of automated systems for collection, storage, analysis or transfer of information;

• comment on the implications for protection of privacy of using or disclosing personal information for record linkage.

Alberta

• The Commissioner may:

• comment on the implications for freedom of information or for protection of personal privacy of proposed legislative schemes or programs of public bodies;

• comment on the implications for protection of personal privacy of using or disclosing personal information for record linkage;

• give advice and recommendations of general application to the head of a public body on matters respecting the rights or obligations of a head under

the Act.

Quebec (Public)

- The annual report of the Commission may contain:

- recommendations in view of promoting the protection of personal information, and the exercise of the right of access to documents, in particular by cultural communities and handicapped persons;

- proposals relating to technical standards of preservation, classification, retrieval and the method of consultation of documents.

Quebec (Private)

- The Commission must, not later than 1 October 1997 and every five years thereafter, submit a report to the Government on the application of the Act.APPENDIX 4 Public Education and Research Functions of Information and Privacy Commissioners

APPENDIX 4 - Public Education and Research Functions of Information and Privacy Commissioners Federal

- The Privacy Commissioner shall, within three months after the termination of each financial year, submit an annual report to Parliament on the activities of the office during that financial year.

- The Privacy Commissioner may, at any time, make a special report to Parliament referring to and commenting on any matter within the scope of the powers, duties, and functions of the Commissioner.

Ontario

- The Commissioner shall make an annual report to the Speaker of the Assembly. This report shall provide a comprehensive review of the effectiveness of the Act and the Municipal Freedom of Information and Privacy Act, 1989, in providing access to information and protection of personal privacy.

- The Commissioner may:

- engage in or commission research into matters affecting the carrying out of the purposes of the Act;

- conduct public education programs and provide information concerning the Act and the Commissioner's role and activities;

- and receive representations from the public concerning the operation of the Act.

B.C.

- The commissioner must report annually to the Speaker of the Legislative Assembly on the work of the commissioner's office, and any complaints or reviews resulting from a decision, act or failure to act of the commissioner as head of a public body.

- The commissioner may:

- inform the public about the Act;

- receive comments from the public concerning the administration of the Act;

- engage in or commission research into anything affecting the achievement of the purposes of the Act.

Alberta

- The Commissioner must report annually to the Speaker of the Legislative Assembly on the work of the Commissioner's office, any complaints or reviews resulting from a decision, act, or failure to act of the Commissioner as head of a public body, and such other matters relating to freedom of information and protection of personal privacy as the Commissioner considers appropriate.

- The Commissioner may:

- conduct investigations to ensure compliance with any provision of the Act or compliance with rules relating to the destruction of records set out in any other enactment of Alberta, or a by-law or other legal instrument by which a local public body acts;

- inform the public about the Act;

- receive comments from the public concerning the administration of the Act;

- engage in or commission research into anything affecting the achievement of the purposes of the Act.

Quebec (Public)

- The Commission shall send to the designated Minister, not later than 30 June each year, a report of its activities for the preceding fiscal year. The report must deal...with how the Act is being observed and the means at the disposal of the Commission to enforce it.

- The report may also contain:

- recommendations in view of promoting the protection of personal information, and the exercise of the right of access to documents, in

particular by cultural communities and handicapped persons;

- proposals relating to technical standards of preservation, classification, retrieval and the method of consultation of documents;

- suggestions from the public on any matter within the competence of the Commission.

Quebec (Private)

- The Commission must, not later than 1 October 1997 and every five years thereafter, submit a report to the Government on the application of the Act.

- Within the year following the tabling of the report before the National Assembly, a designated committee must examine the advisability of maintaining the Act in force as it stands, or...of amending it, and shall hear the representations of interested persons and bodies on such matters.APPENDIX 5 Terms of Office for Information and Privacy Commissioners

APPENDIX 5 - Terms of Office for Information and Privacy Commissioners Federal

- The Privacy Commissioner holds office during good behaviour for a term of seven years, but may be removed by the Governor in Council at any time on address of the Senate and House of Commons

Ontario

- The Commissioner shall hold office for a term of five years and may be reappointed for a further term or terms, but is removable at any time for cause by the Lieutenant Governor in Council on the address of the Assembly.

B.C.

- The commissioner holds office for a term of 6 years and is not eligible to be reappointed as commissioner.

Alberta

- The Commissioner holds office for a term of 5 years.

- A person holding office as Commissioner continues to hold office after the expiry of that person's term of office until that person is reappointed, a successor is appointed or a period of 6 months has expired, whichever occurs first.

Quebec (Public)

- The term of office of the members of the Commission is not over five years.

- In no case may the members of the Commission be appointed for more than two consecutive full terms.

Quebec (Private)

- The Commission d'acces a l'information is established by the Act respecting Access to documents held by public bodies and the Protection of personal information.

Task Force Home Page

Help What's New Sitemap Feedback About Us Français Top of Page

Canada

Last modified - 10/04/2000

Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

Colin J. Bennett
Professeur agrégé
Département de sciences politiques
Université de Victoria
Victoria (C.-B.) V8W 3P5
CANADA

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
  - La réception, la vérification et l'approbation des codes de protection de la vie privée
  - Plaintes : réception, enquête et règlement
  - Pouvoirs de vérification
  - Pouvoirs d'exécution
  - Conseils au sujet des répercussions des technologies nouvelles sur la protection de la vie privée
  - Éducation publique et recherche
  - Sanctions et recours
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexe 1

- Annexe 2
- Annexe 3
- Annexe 4
- Annexe 5

- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000

Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexes

INTRODUCTION

Le 25 mars 1996, Industrie Canada a tenu un atelier axé sur le thème de l'analyse de la fonction de surveillance de la protection des données personnelles au sein du marché. À la séance du matin, des représentants des Pays-Bas, de la Nouvelle-Zélande, du Québec, de Hong Kong et des États-Unis ont expliqué de quelle façon les dispositions législatives en matière de protection des données sont appliquées et exécutées au sein de leurs sociétés respectives. Dans l'après-midi, les participants ont tenu une table ronde sur la mise en œuvre d'une politique de protection des données dans le contexte canadien. Les représentants du Canada comprenaient des hauts fonctionnaires de ministères fédéraux, du Commissariat à la protection de la vie privée (CPVP) et des bureaux provinciaux de l'ombudsman et du commissaire à l'information et à la protection de la vie privée, ainsi que des responsables de l'Association canadienne de normalisation (CSA).

Industrie Canada m'a demandé d'agir comme rapporteur pour cet atelier et de rédiger un rapport sur les activités de la journée. Cependant, les opinions exprimées dans le présent document ne sont pas un strict compte rendu de tout ce qui a été dit à l'atelier, et aucune d'entre elles n'est attribuée à un quelconque des participants. Le lecteur trouvera plutôt dans les pages qui suivent une série de réflexions personnelles sur les diverses possibilités d'étendre au secteur privé les règles qui régissent la protection de la vie privée, à la lumière des échanges fort instructifs qui ont eu lieu à l'atelier. Les opinions exprimées ne sont que les miennes, même si elles ont été façonnées par de nombreuses conversations que j'ai eues avec des spécialistes et des fonctionnaires avant et après l'atelier du 25 mars.

Ce document se fonde aussi sur les travaux que j'ai moi-même réalisés antérieurement sur la mise en œuvre de politiques de protection de la vie privée dans d'autres pays, et surtout sur le rapport intitulé *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, de même que sur les recherches menées sur la mise en œuvre du Code type pour la protection des renseignements personnels (Q830) de l'Association canadienne de normalisation. Le document prend également appui sur d'autres analyses comparatives et canadiennes au sujet de la mise en œuvre de politiques de protection de la vie privée . Plus particulièrement, le rapport qu'Ian Lawson a publié en 1995 expose une série complète d'options de réglementation relatives à la protection de la vie privée sur l'autoroute de l'information. Le présent document vise à restreindre le champ d'étude, et à se concentrer sur les options réglementaires qui s'avèrent les plus pratiques pour le Canada.

Bien qu'il existe amplement de possibilités de tirer des leçons de ce qui se fait au Canada et à l'étranger, nous ne partons pas de zéro. Il existe des lois qui visent le secteur public à l'échelon fédéral, ainsi que dans la plupart des provinces. Au Québec, le projet de loi 68 est le seul texte législatif au Canada qui réglemente les pratiques du secteur privé. Chacune de ces lois accorde un éventail différent de pouvoirs et de responsabilités aux bureaux respectifs des commissaires à l'information et à la protection de la vie privée (voir les annexes). Il y a en outre une foule d'autres dispositions dans des lois provinciales et fédérales qui se rapportent à la collecte, au stockage, au traitement et à la transmission de données personnelles. Bien des entreprises ont également créé des « codes de pratique » volontaires. Il est impossible de faire table rase et d'établir, à partir de zéro, un régime de protection de la vie privée. Le processus d'élaboration d'une politique sera forcément progressif et devra s'appuyer sur les instruments et les dispositions qui existent déjà.

En outre, le document ne s'étendra pas sur la question complexe des pouvoirs constitutionnels du gouvernement fédéral et des provinces. Dans une large mesure, les questions relatives aux mécanismes appropriés de surveillance et d'observation s'appliqueront, indépendamment du fait que l'on crée des dispositions législatives qui sont d'une large portée, ou qui s'appliquent de façon plus étroite aux entités assujetties à la réglementation fédérale. Le présent document traite des fonctions qu'il est nécessaire d'exécuter dans n'importe quel régime efficace de protection des données personnelles. Ces fonctions devront être soigneusement analysées, qu'elles soient exécutées à l'échelon fédéral et/ou à l'échelon provincial, ou sur une base générale ou sectorielle. Il est question dans ce document du degré de réglementation. Il continuera de survenir des conflits de compétence, peu importe le régime législatif ou d'autoréglementation qui sera retenu.

Je suis donc redevable aux personnes qui ont pris part à l'atelier du 25 mars. Ce document ne peut présenter aucun consensus sur les résultats de cette réunion, mais j'espère néanmoins que les personnes présentes y reconnaîtront les thèmes et les points les plus importants dont il a été question à cette occasion. Je remercie aussi Ritu Mahil de m'avoir aidé sur le plan des recherches.

- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000

Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexes

La norme nationale en matière de protection de la vie privée

Dans le rapport qu'il a publié en 1995, le Comité consultatif sur l'autoroute de l'information (CCAI) conseillait au gouvernement fédéral de :

créer des règles du jeu équitables pour la protection des renseignements personnels sur l'autoroute de l'information en élaborant et en mettant en œuvre un cadre législatif souple pour les secteurs public et privé. Les mesures législatives adoptées exigeraient que les divers secteurs et organismes respectent la norme fixée par le code type de la CSA tout en leur laissant la possibilité d'améliorer leurs propres codes.

Dans ce rapport, il était en outre recommandé au gouvernement fédéral d'« étudier, de concert avec le groupe de travail de la CSA sur la vie privée et d'autres parties intéressées, l'élaboration de mécanismes efficaces de

surveillance et d'application ». Le présent document est une contribution à ce travail.

Le 23 mai, le ministre de l'Industrie, John Manley, a publié la réponse du gouvernement au rapport du CCAI, réponse dans laquelle il a été conclu que « le droit à la protection des renseignements personnels doit être reconnu dans la loi, surtout dans un monde électronique de bases de données privées où il est très facile de recueillir et d'exploiter des renseignements sur une personne ». Par conséquent :

Afin d'encourager les entreprises et les consommateurs à avoir confiance dans l'autoroute de l'information, les ministres de l'Industrie et de la Justice, après avoir consulté les provinces et les autres intervenants, proposeront une loi-cadre régissant la protection des renseignements personnels dans le secteur privé.

Dans sa réponse, le gouvernement mentionne expressément le Code type pour la protection des renseignements personnels de l'Association canadienne de normalisation comme cadre législatif. Les principes énumérés ci-dessous, lesquels ont obtenu un large appui de la part de représentants de l'État, de l'industrie et d'associations de consommateurs, représentent un consensus important au sujet des principes fondamentaux d'une politique en matière de protection de la vie privée :

- *Responsabilité*

Un organisme est responsable des renseignements personnels dont il a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessus.

- *Détermination des fins de la collecte des renseignements*

Les fins pour lesquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisme avant ou au moment de la collecte.

- *Consentement*

Toute personne doit être informée et consentir à toute collecte, utilisation ou communication de renseignements personnels qui la concernent, à moins qu'il ne soit pas approprié de le faire.

- *Limitation de la collecte*

L'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

- *Limitation de l'utilisation, de la communication et de la conservation*

Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées.

- *Exactitude*

Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils sont utilisés.

- *Mesures de sécurité*

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

- *Transparence*

Un organisme doit mettre à la disposition de toute personne des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

- *Accès aux renseignements personnels*

Un organisme doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera possible de contester l'exactitude et l'état complet des renseignements et y faire apporter les corrections nécessaires.

- *Possibilité de porter plainte contre le non-respect des principes*

Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec le ou les individus responsables de les faire respecter au sein de l'organisme concerné.

Toute politique nationale en matière de protection de la vie privée devrait avoir pour objectif de mettre en œuvre ces principes dans l'ensemble des organismes qui traitent des données personnelles (dans le secteur public comme dans le secteur privé).

Cet objectif nécessite la prise de mesures volontaires « du bas vers le haut », de même que des mesures réglementaires du haut vers le bas. Il existe une gamme d'outils au sein du répertoire d'instruments possibles. Quatre sont décrits dans le document qu'Industrie Canada a publié en 1994 sous le titre de *La protection de la vie privée et l'autoroute canadienne de l'information : les lois et la réglementation, les codes et les normes volontaires, les solutions technologiques, et l'éducation des consommateurs*. Bien que le présent document s'attache à la relation qui existe entre les lois, les règlements, les codes et les normes, il ne faut jamais perdre de vue que les technologies liées à la protection de la vie privée (l'encryptage à clé publique en est un exemple) ont un rôle capital à jouer au sein de n'importe quelle politique régissant la protection de la vie privée. De plus, aucune politique ne sera fructueuse sans les interventions de particuliers informés et vigilants. Chacun de ces quatre outils contribue à ce qui a été appelé une « mosaïque de solutions » . Chacun est indispensable pour protéger la vie privée sur l'autoroute de l'information, et aucun n'est suffisant.

- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000

Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexes

La valeur de la norme relative à la protection de la vie privée

En ce qui concerne la protection de la vie privée, le statu quo a été qualifié de mesure « trop disparate ». L'existence au Québec d'une loi exhaustive en matière de protection des données, qui vise l'ensemble des organisations du secteur privé de cette province, fait contraste avec le fatras de codes volontaires et de mesures législatives isolées que l'on retrouve dans le reste du pays. Réagissant, en partie, à cette incohérence, l'Association canadienne de normalisation (CSA) a récemment établi un Code pour la protection des renseignements personnels, en association avec divers intervenants de l'État, de groupes de consommateurs et de secteurs clés de l'industrie (banques, télécommunications, assurances, télémarketing et agences d'informations financières). Ce Code, ratifié sans dissidence aucune en septembre 1995 et diffusé en mars 1996, a été conçu pour uniformiser d'une certaine façon les politiques et les pratiques en matière de protection des données au sein du secteur privé canadien.

À première vue, le Code type de la CSA peut sembler être une version canadienne des Directives de l'OCDE - une réorganisation des principes clés et une adaptation de ces dernières au contexte canadien. Il ne s'agit, pour l'heure, que de cela : un modèle que n'importe quel organisme peut utiliser et adapter en fonction des circonstances qui lui sont propres. Mais il fait toutefois l'objet d'un consensus fort important de la part des principaux intervenants. En outre, il a sans aucun doute été fort utile aux entités qui ont pris part au processus pour réfléchir, à partir de zéro, au problème que pose la question de la protection de la vie privée, de même que pour s'attaquer à ces questions complexes.

Bien qu'aucune décision n'ait encore été prise au sujet des mécanismes de mise en œuvre et de surveillance, le Code type de la CSA est une « norme » qui pourrait être soumise aux mêmes modalités de certification et d'adhésion que celles que l'on applique pour d'autres normes. Bien sûr, la protection de la vie privée n'est pas le genre de norme « stricte » que l'on applique habituellement au sein de l'industrie manufacturière. Elle présente néanmoins certains parallèles avec l'éventail des « normes de gestion de la qualité » que comporte la série ISO-9000 et qui se propagent rapidement dans le secteur privé au Canada et aux États-Unis, ainsi qu'avec les normes environnementales de la série ISO-14000. C'est donc dire qu'à l'instar d'une entreprise qui pourrait être contrainte d'adhérer à la norme ISO-9000 pour convaincre sa clientèle qu'elle a adopté un certain niveau d'« assurance de la qualité », il serait possible d'établir le même système d'accréditation en rapport avec la norme relative à la protection de la vie privée, qui obligerait à protéger les données de manière efficace au sein du marché canadien ou international. Le prix à payer pour être inscrit serait la soumission à des vérifications indépendantes et régulières des mesures prises en matière de protection de la vie privée.

Il va sans dire que l'on ne s'attendrait pas à ce que toutes les entreprises se lancent dans le genre d'efforts et de dépenses qu'occasionne l'adhésion à la norme ISO-9000. En ce qui concerne la protection de la vie privée, le régime d'adhésion exigerait aussi des modalités qui s'appliquent aux petites entreprises. Dans le cadre de ce régime, il faut trouver un juste équilibre entre, d'une part, le fait d'encourager l'adhésion et, d'autre part, celui de prévenir les prétentions symboliques concernant les politiques et les pratiques qui sont appliquées. Il exige aussi un mécanisme de publicité approprié, de sorte que les consommateurs puissent savoir qui adhère à la norme et qui n'y adhère pas. Il faudrait que le régime d'adhésion soit assorti d'une liste d'organismes admis, comme un registre de protection de la vie privée.

Si l'on établit un processus d'adhésion crédible, le Code type de la CSA cesse d'être un mécanisme « volontaire ». Les organismes auraient à produire un code et une série connexe de directives opérationnelles, et seraient assujettis à une vérification régulière et indépendante de leurs pratiques. Le régime établirait un système de vérification plus cohérent et plus crédible que celui qui a cours à l'heure actuelle. Il pourrait satisfaire à des exigences internationales et contractuelles. Il pourrait constituer un moyen plus commun et plus cohérent d'observer et d'évaluer les pratiques des entreprises. Un tel système serait capable de contrôler les prétentions faites par les organismes au sujet de leurs politiques et de leurs pratiques.

J'ai suggéré que la norme relative à la protection de la vie privée s'étende à l'ensemble du marché au moyen d'un certain nombre de mesures différentes d'incitation à l'adhésion : par la persuasion, par le désir d'éviter toute publicité

négative, par le désir d'obtenir un avantage concurrentiel, en faisant référence à la norme dans un contrat privé, en adhérant à la norme relative à la protection de la vie privée de pair avec la norme ISO-9000, en faisant référence à la norme lorsque l'État « sous-traite » des services de traitement de données, par la pression exercée par des organismes de financement de recherches, par la réglementation de la circulation interprovinciale de données dans le projet de loi 68 du Québec, ainsi que par l'emploi des dispositions relatives au « niveau de protection adéquat » que font les instances européennes chargées de la protection des données. Les organismes de réglementation canadiens et étrangers pourraient insister pour que la réception de données personnelles au Canada s'accompagne d'une adhésion au Code type de la CSA.

Comme nous l'avons vu plus tôt, le fait d'adhérer au Code type de la CSA serait un moyen plus efficace d'évaluer les pratiques en matière de renseignements personnels. Cette mesure permettrait de sensibiliser davantage les consommateurs à la question. Elle pourrait hausser les niveaux de responsabilité et de reddition de comptes au sein des entreprises canadiennes. Elle permettrait peut-être de contrôler davantage, et mieux, les mesures de protection de la vie privée. Mais le processus serait quand même progressif et fragmentaire; il ne donnerait jamais lieu à la sorte de norme juridique uniforme dont on a besoin au Canada, la protection uniforme demandée par le commissaire fédéral à la protection de la vie privée.

- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000

Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexes

La valeur ajoutée des mesures législatives concernant la protection des données

Si l'on fait abstraction des dilemmes constitutionnels particuliers qui se posent au Canada, qu'ajouterait un régime légal à la solution d'élaborer des normes contrôlées par un régime d'adhésion administré par un organisme agréé d'adhésion ? Il existe cinq arguments convaincants.

Premièrement, seule une loi peut énoncer les normes de la collectivité, la limite qu'aucun organisme ne devrait pouvoir franchir. C'est à cela que songe Bruce Phillips lorsqu'il fait valoir ce qui suit : « [à] moins qu'on n'adopte des règles intégrales de gestion sensée de la " circulation ", les premières victimes de l'autoroute de l'information seront notre vie privée et notre dignité ». Cette métaphore de l'« autoroute de l'information » mène naturellement à l'argument indéniable selon lequel il doit exister un « code de la route » cohérent. Pour bien des entreprises, le code de la route pourrait les

intéresser à créer des « règles du jeu équitables » - un ensemble clair et cohérent de règles relatives à la protection de la vie privée, qui s'applique à l'ensemble du marché canadien.

Une loi ne fournit pas nécessairement cette norme. Bien trop souvent, nous rappelle Oscar Gandy, nous avons tendance à parler de la loi comme de l'instrument impartial qui permet de s'assurer que sont protégées et garanties les valeurs universelles revendiquées pour une société quelconque. N'importe quel tenant d'un régime légal doit reconnaître les vastes inégalités que comporte l'application d'une loi, surtout lorsque l'on s'en sert comme une arme stratégique plutôt que comme l'expression d'une vision morale fondamentale, une série de principes directeurs qui servent de fondements aux rapports entre les gens.

Deuxièmement, il y a peu de chances que ce « code de la route » soit appliqué de manière impartiale, sous la direction d'une « police » impartiale. Selon le Code type de la CSA, chaque organisme doit désigner une personne chargée de veiller à ce que l'on se conforme à la norme, et les organismes doivent clairement indiquer comment les consommateurs peuvent contester la façon dont on se conforme aux principes établis (principes 1 et 10). Dans les circonstances actuelles, le mécanisme supérieur de règlement des plaintes que l'on retrouve dans la plupart des secteurs se situe au sein de l'entreprise qui traite les données personnelles. Seule une loi peut créer un arbitre définitif, qui se trouve à l'extérieur de l'organisme en cause. Seule une loi peut faire participer les institutions qui, à ce jour, possèdent la meilleure expérience qui soit dans le domaine du règlement des plaintes relatives à la protection de la vie privée au Canada : les bureaux des commissaires fédéral et provinciaux à l'information et à la protection de la vie privée.

Troisièmement, seule une loi permet d'amener les éléments récalcitrants dans le droit chemin. Quelle que soit l'efficacité avec laquelle le Code type de la CSA peut réglementer les pratiques des entreprises les plus sérieuses, il y aura toujours une minorité qui percevra un avantage concurrentiel dans le fait de traiter des données personnelles d'une manière contraire à la norme. Il ne fait aucun doute que c'est la crainte de l'ACMD de voir ternir l'image de ses membres sérieux par une minorité de non-membres qui l'a incitée à demander que l'on adopte une loi nationale fondée sur la norme de la CSA. Voilà un geste fascinant; il dénote que jusqu'à un certain point dans certains secteurs l'adoption d'une loi devient la solution de rechange acceptable à une mauvaise publicité constante.

Quatrièmement, il est possible d'invoquer un argument économique. Comme l'a fait valoir Ian Lawson : « [d]ans la mesure où une entreprise obtient et utilise les renseignements personnels sans mécanisme de marché pour régir l'échange, elle est un resquilleur classique de l'économie. Elle consomme une ressource qui est un bien commun sans supporter les effets externes liés à son extraction et à son usage ». C'est donc dire que lorsqu'un organisme profite de l'usage des informations, soit personnellement soit en échangeant ces dernières avec une tierce partie, le fournisseur initial des informations n'en retire aucun avantage. Cette situation perdure parce que bien des entreprises ne sont pas disposées à faire preuve de transparence au sujet de leurs pratiques et à établir des mécanismes visant à obtenir un consentement éclairé lorsqu'elles désirent utiliser des informations personnelles à des « fins secondaires ». Les entreprises demeurent des « resquilleurs » tant que les individus sont maintenus dans l'ignorance quant à la façon dont on utilise et divulgue les informations qui les concernent.

Selon les théories économiques classiques, il est possible de corriger un marché imparfait de deux façons. Premièrement, il est possible de donner une certaine valeur aux informations personnelles de manière à mieux répartir les coûts et les avantages des opérations qui sont faites. Quelques propositions ont été formulées à propos de l'établissement de solutions fondées sur le marché en vue de corriger ce déséquilibre; toutes ces propositions reposent sur des régimes qui permettent d'accorder aux particuliers des droits de propriété sur les informations les concernant, ainsi qu'un dédommagement convenable lorsque ces informations servent à des fins autres que celles pour lesquelles elles ont été fournies au départ. L'autre solution consiste à intervenir par voie réglementaire pour rectifier le déséquilibre du marché. Il est contestable, bien sûr, que les théories économiques aient un rôle quelconque à jouer dans la protection d'un droit fondamental de la personne. Néanmoins, même d'après les principes du raisonnement économique néoclassique, il est difficile de résister aux arguments en faveur d'une intervention de nature réglementaire.

Cinquièmement, seule la loi est capable d'harmoniser les normes du secteur public et du secteur privé. Il est de plus en plus difficile de déterminer où prend fin le secteur « public » et où commence le secteur « privé ». Les questions soulevées au sujet de l'application et de la signification des dispositions en matière de protection de la vie privée que comportent la *Loi sur la protection des renseignements personnels* du gouvernement fédéral et les lois provinciales connexes se répercuteront de plus en plus sur les pratiques du secteur privé. On peut s'attendre aussi à ce que l'attention accrue que recevront dans les médias les questions relatives à la protection de la vie privée par suite des efforts des commissaires à la protection de la vie privée continue d'avoir un effet d'entraînement. La nécessité d'assurer une « protection uniforme » entre le secteur privé et le secteur public est l'un des facteurs clés qui sous-tend l'adoption de la *Privacy Act* en Nouvelle-Zélande.

La distinction est également minée par les efforts qui sont faits pour privatiser ou décentraliser les fonctions de l'État. C'est ainsi que des organismes « privés » accomplissent un nombre croissant de fonctions « publiques », et requièrent souvent pour ce faire des données « publiques ». En voici quelques exemples : l'utilisation de cartes à puce et de machines NTA pour verser les prestations de l'État; l'appariement de renseignements sur les assistés sociaux avec des documents bancaires ou financiers afin de vérifier l'admissibilité de ces personnes, l'échange de renseignements personnels que possède l'État afin d'améliorer les recettes, l'utilisation de rapports de crédit pour vérifier la sécurité, et ainsi de suite. Vu l'omniprésence et la souplesse des nouvelles technologies, il sera de plus en plus ardu de déterminer quelles données se trouvent « dans » le secteur public, et lesquelles se situent « dans » le secteur privé.

La dernière raison - la moins importante - concerne l'interprétation de l'article 25 de la nouvelle Directive européenne sur la protection des données :

Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.

Indépendamment des dispositions de l'article 26 selon lesquelles il peut être tenu compte des « règles professionnelles et [des] mesures de sécurité qui [...] sont respectées » au moment de déterminer le « niveau de protection adéquat », l'article 25 voudrait dire peut-être que les organismes de réglementation européens pourraient, légitimement, interrompre la circulation de données vers n'importe quelle partie du Canada, exception faite du Québec, à moins que des mesures de protection légales soient établies. Un « niveau de protection adéquat » pourrait être interprété comme un régime législatif, supervisé par une « instance de surveillance » indépendante. Il convient de noter, à tout le moins, qu'il est nécessaire de se conformer à toute règle de nature professionnelle (comme un code de pratique). N'importe quel système canadien de protection des données doit montrer qu'il est mis en œuvre de manière sérieuse et efficace.

- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000

Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexes

Légiférer en fonction de la norme

Contrairement aux codes de pratique volontaires, il est possible de faire référence dans la loi à la norme de la CSA, et c'est le cas, dans une loi fédérale ou une loi provinciale, du tiers environ des normes publiées par cet organisme. La plupart de ces dernières sont liées aux normes techniques qui s'appliquent aux produits qu'acquiert l'État. De plus en plus toutefois, on applique des normes de rendement comme celles qui s'appliquent à la gestion de la qualité ou à la protection de l'environnement pour mettre en œuvre une loi, un règlement et une ordonnance judiciaire. Rien n'empêche les autorités fédérales ou provinciales d'utiliser de la même façon la norme Q830.

Dans son rapport, le Comité consultatif sur l'autoroute de l'information envisage toutefois une démarche plus exhaustive - un « cadre législatif souple pour les secteurs public et privé. Les mesures législatives adoptées exigeraient que les divers secteurs et organismes respectent la norme fixée

par le code type de la CSA tout en leur laissant la possibilité d'améliorer leurs propres codes ». Cette recommandation semble envisager l'établissement d'une loi « cadre » à l'échelon fédéral; un énoncé de principes et d'obligations dans lequel les fonctions relatives au règlement des plaintes, aux enquêtes, aux mesures de contrôle, etc. doivent faire l'objet d'une analyse supplémentaire menée « de concert avec le groupe de travail de la CSA sur la vie privée ». Mais il y a eu un certain nombre d'interprétations différentes de la pensée du CCAI et de ce que cela veut dire que de « légiférer en fonction de la norme ».

Ainsi, l'Association canadienne du marketing direct (ACMD) a exhorté le ministre Manley à :

[TRADUCTION] « [...] présenter au Parlement une loi fédérale cadre obligeant chaque secteur de l'industrie à établir, à l'égard de la protection de la vie privée, son propre code particulier qui satisfasse à une norme nationale. Nous ne croyons pas que cette loi doit être complexe, non plus que coûteuse à appliquer. Nous suggérons un modèle semblable à celui de la Loi canadienne sur la santé, qui fixe des normes nationales minimales, tout en permettant à chaque province de créer et d'administrer son propre système de soins de santé pour répondre aux besoins qui lui sont propres. »

L'ACMD explique ensuite que [TRADUCTION] « chaque code refléterait les besoins du secteur particulier et satisferait aux normes fixées par l'OCDE et/ou les projets de codes de la CSA ». En outre, cet organisme s'inquiète aussi de ce que [TRADUCTION] « les pouvoirs réglementaires pourraient servir à rendre les principes plus stricts. Nous croyons que l'idée de permettre aux industries de créer des normes qui protègent la vie privée et répondent à leurs besoins particuliers préviendra toute ingérence réglementaire excessive ». L'ACMD déléguerait au Commissaire fédéral à la protection de la vie privée une petite fonction de règlement des plaintes.

Il y a une distinction importante à faire entre le volontarisme et l'autoréglementation. Le premier implique que la politique de l'État doit demeurer indifférente aux politiques et aux pratiques poursuivies. L'État doit simplement faire confiance à l'entreprise pour ce qui est de poursuivre des pratiques favorables à la protection de la vie privée, mais il n'est nullement intéressé à fixer une norme générale. Telle est, à ce jour, la position des gouvernements fédéraux du Canada et des États-Unis. En revanche, un régime d'autoréglementation crée en droit la norme applicable et accorde aux entreprises le pouvoir de réglementer leurs propres pratiques. La principale différence est qu'une norme législative est fixée et que les individus et les organismes savent que, lorsque l'autoréglementation échoue, les instruments de principe établis en vertu de la loi peuvent intervenir.

Le Commissaire fédéral à la protection de la vie privée voit les choses d'un oeil légèrement différent, et laisse entendre que le Code type de la CSA pourrait constituer une modification à la Loi sur la protection des renseignements personnels. Cette option est attirante pour le Commissaire, car elle intégrerait en droit une série de règles conçues par un comité représentant un vaste échantillon d'entreprises privées au Canada. Mais le Commissaire ne dit rien au sujet des codes. Selon lui, l'avantage qu'il y a à légiférer en fonction de la norme est que l'« observation de la norme de la CSA deviendrait une obligation légale appuyée par un système de surveillance indépendant ».

Ian Lawson reconnaît lui aussi le consensus unique qui se dégage entre l'État,

les consommateurs et les intervenants de l'industrie, et que cette situation se reflète dans le Code type de la CSA. Selon lui, le but premier du Code est d'être adopté par référence sous la forme d'une norme législative que doit observer le secteur privé s'il désire utiliser des renseignements personnels sur l'autoroute de l'information ».

Lawson décrit trois options possibles pour la création de mesures réglementaires basées sur l'application de normes. Selon sa « version légère », le gouvernement fédéral édicte une loi-cadre qui dispose que les utilisateurs de données doivent se conformer au Code type de la CSA en établissant un code approprié qui satisfasse à la norme de l'industrie. Le modèle dépendrait entièrement de la CSA en tant qu'instrument de contrôle, et ne comporte aucune fonction évidente (à part celle de la persuasion) pour les commissaires à la protection de la vie privée.

Selon sa « version moyenne », les commissaires à la protection de la vie privée seraient chargés de recevoir les plaintes des consommateurs quant à la façon dont l'utilisateur des données se conforme à son code. Les commissaires appliquent les techniques existantes de solution de problèmes, dont l'éducation, la persuasion et la médiation. Cela ajoute donc un niveau de surveillance au Code type de la CSA, en plus de tout processus de vérification et d'adhésion établi par l'entremise d'un registraire agréé. Cette solution ajoute peut-être un moyen de recours plus cohérent et plus précis pour l'individu qui s'estime lésé, et confie la responsabilité générale des activités de surveillance aux institutions qui sont exclusivement chargées de la protection de la vie privée et qui sont compétentes en ce domaine.

Selon la « version lourde » de Lawson, les commissaires à la protection de la vie privée régleraient les plaintes, mais seraient également habilités à rendre des ordonnances obligeant les utilisateurs de données à se conformer à leur code; le fait de ne pas se soumettre à ces ordonnances constituerait une infraction criminelle. La loi établirait aussi une responsabilité civile pour les cas où un utilisateur de données omet de se conformer à son code. Ce n'est que dans la « version lourde » de Lawson que l'adhésion serait soutenue par une série de droits exécutables légalement, et soumis à la surveillance générale des commissaires à la protection de la vie privée. Ce n'est aussi que dans cette version que serait établi un système de protection des données, qui ferait peser sur le problème l'éventail complet des mécanismes de conformité.

Le reste du présent document est fondé sur l'analyse de Lawson, et traite de manière plus détaillée des fonctions de surveillance dans le cadre d'un système au sein duquel il est fait référence, dans une loi fédérale ou provinciale, au Code type de la CSA. S'il est dit dans la loi qu'une entreprise exerçant ses activités au Canada doit se conformer au Code si elle veut utiliser des renseignements personnels sur l'autoroute de l'information, quelles responsabilités et obligations supplémentaires faut-il assigner?

- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000

Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexes

Les fonctions de surveillance

Une approche fonctionnelle de l'analyse des politiques commence par un énoncé des fonctions qui pourraient être exécutées au sein de n'importe quelle politique publique, et ne considère qu'ensuite les organismes publics et privés qui sont susceptibles d'exécuter ces fonctions. Les discussions qui ont eu lieu à l'atelier tenu le 25 mars ont été structurées d'après les fonctions suivantes : la réception, la vérification et l'approbation de codes de protection de la vie privée; la réception des plaintes, les enquêtes menées sur ces dernières et leur règlement; les pouvoirs d'exécution; le contrôle des organismes; les conseils sur les répercussions des nouvelles pratiques technologiques sur la protection de la vie privée; l'éducation et la recherche; ainsi que les recours et les sanctions. L'analyse exposée ci-après suit le même plan.

- La réception, la vérification et l'approbation des codes de protection de la vie privée

- Plaintes : réception, enquête et règlement
- Pouvoirs de vérification
- Pouvoirs d'exécution
- Conseils au sujet des répercussions des technologies nouvelles sur la protection de la vie privée
- Éducation publique et recherche
- Sanctions et recours

- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000

Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexes

Sommaire : Les éléments d'un système de surveillance au Canada

Il convient maintenant de résumer l'analyse en vue de tirer quelques conclusions provisoires au sujet des éléments que pourrait comporter un système de surveillance de la protection des renseignements personnels au sein du secteur privé canadien :

- Les gouvernements fédéral et provinciaux doivent appliquer l'éventail complet des instruments de principe qui sont disponibles au problème que pose la protection de la vie privée : des codes d'autoréglementation, des mesures législatives, des technologies visant à protéger la vie privée, ainsi que de meilleurs programmes d'éducation des consommateurs. Il s'agit là des instruments de principe. Ces derniers ne s'excluent pas les uns les autres; il est nécessaire de tous les utiliser.

- Les trois années de négociation entourant la norme CSA représentent une étape cruciale dans le processus d'élaboration d'une politique. Le consensus voulu a été obtenu. Tout régime législatif doit être fondé sur cette mesure d'accommodement.

- Une loi sur la protection de la vie privée au sein du secteur privé ne doit pas être nécessairement fastidieuse ou exagérément compliquée. Le Canada devrait éviter de recourir aux systèmes d'homologation et d'enregistrement coûteux et bureaucratiques qui ont été établis dans certaines sociétés européennes.

- En revanche, une loi non dotée d'un mécanisme efficace de vérification de la conformité peut être pire que l'absence d'une loi quelconque, et ne serait pas considérée comme « adéquate » pour satisfaire aux exigences des normes européennes.

- Les organismes centraux de surveillance devraient être les commissariats fédéral et provinciaux à l'information et à la protection de la vie privée (là où il en existe). Ces bureaux jouissent d'une certaine indépendance, crédibilité et compétence. Ils sont situés de manière unique au sein du milieu réglementaire pour superviser les dispositions législatives qui régissent le secteur privé, et régler des questions qui couvrent la ligne de partage entre le secteur public et le secteur privé.

- Tout régime législatif doit arriver à un équilibre des responsabilités pour ce qui est des fonctions suivantes : règlement des plaintes et médiation; enquête sur les plaintes; vérifications; conseils au sujet des répercussions de technologies nouvelles sur la protection de la vie privée; promotion de codes de pratique; éducation publique; recherche. Les recours les plus efficaces peuvent être ceux qui sont de nature générale et proactive, plutôt que réactive.

- Le règlement des différends devrait susciter le moins de litiges possible, et ne s'appliquer qu'après que toutes les autres voies ont été épuisées. Les entreprises voudront que l'on règle rapidement et de façon prévisible les problèmes liés à la protection de la vie privée. Il sera peut-être bon qu'un tribunal fédéral ou provincial spécialisé dans le domaine de la protection de la vie privée règle les différends relatifs aux questions liées au secteur privé.

- L'adhésion au Code type de la CSA constitue un mécanisme d'exécution crucial, dénué de tout régime réglementaire éventuel. Le fait d'adhérer à cette norme privée peut compléter la quasi-totalité des dispositions actuelles ou futures, contractuelles ou réglementaires, provinciales ou fédérales, sectorielles ou générales, qui ont trait à la protection des données personnelles. Ce code peut servir à récompenser les bonnes pratiques, et ramener les récalcitrants dans le droit chemin.

- Les codes de protection de la vie privée continueront manifestement de jouer un rôle important au sein de n'importe quel régime législatif. Le processus d'adhésion aux normes peut libérer les organismes de réglementation de la tâche de contrôler et de vérifier la teneur des codes de protection de la vie privée. Un régime qui oblige tous les organismes à établir un code de protection de la vie privée serait inutilement fastidieux et coûteux. Par conséquent, il faudrait continuer d'établir des codes en réponse à la

demande du marché et aux pressions des consommateurs, mais uniquement dans des circonstances spéciales, en réponse à une décision de nature réglementaire.

- L'expérience acquise à l'étranger donne à penser que les codes de pratique qui jouissent d'une forme quelconque de statut juridique (allant au-delà de la valeur probante) sont difficiles à négocier et fastidieux. Il faudrait inciter à établir des codes de protection de la vie privée, et ces derniers devraient prendre pour modèle la norme CSA. Cependant, dans le cadre d'un régime législatif, il ne faudrait pas leur accorder un « sceau d'approbation » officiel, ni le pouvoir de nuancer les dispositions de la loi. Cependant, les commissaires et les tribunaux peuvent tenir compte du fait que l'on se conforme à un code approuvé par la CSA au moment de déterminer s'il y a eu infraction ou non aux principes régissant la protection de la vie privée.

- L'expérience démontre que les sanctions revêtant la forme d'une amende ne sont pas une mesure incitative importante. Les recours en matière civile sont également inefficaces car il est difficile de prouver qu'un traitement délibérément illicite de données personnelles a causé des dommages réels.

- Dans le contexte de la surveillance du secteur privé, la menace d'une publicité négative peut contribuer dans une grande mesure à garantir le respect des principes qui régissent la protection des données. Cette mesure incitative a probablement plus de poids dans le secteur privé que dans le secteur public. Le processus de rapports publics est donc d'une importance cruciale dans n'importe quel modèle de surveillance.

- Il est possible que la sanction la plus efficace soit un pouvoir réglementaire d'ordonner que l'on adhère à la norme établie. Ainsi, lorsqu'une série de plaintes seraient déposées au sujet d'une entreprise particulière, les commissaires à la protection de la vie privée ou les tribunaux pourraient obliger cette dernière à adhérer à la norme, ce qui déclencherait l'établissement d'un code et la mise en marche d'un processus de vérification, dont les coûts seraient transmis à l'utilisateur des données.

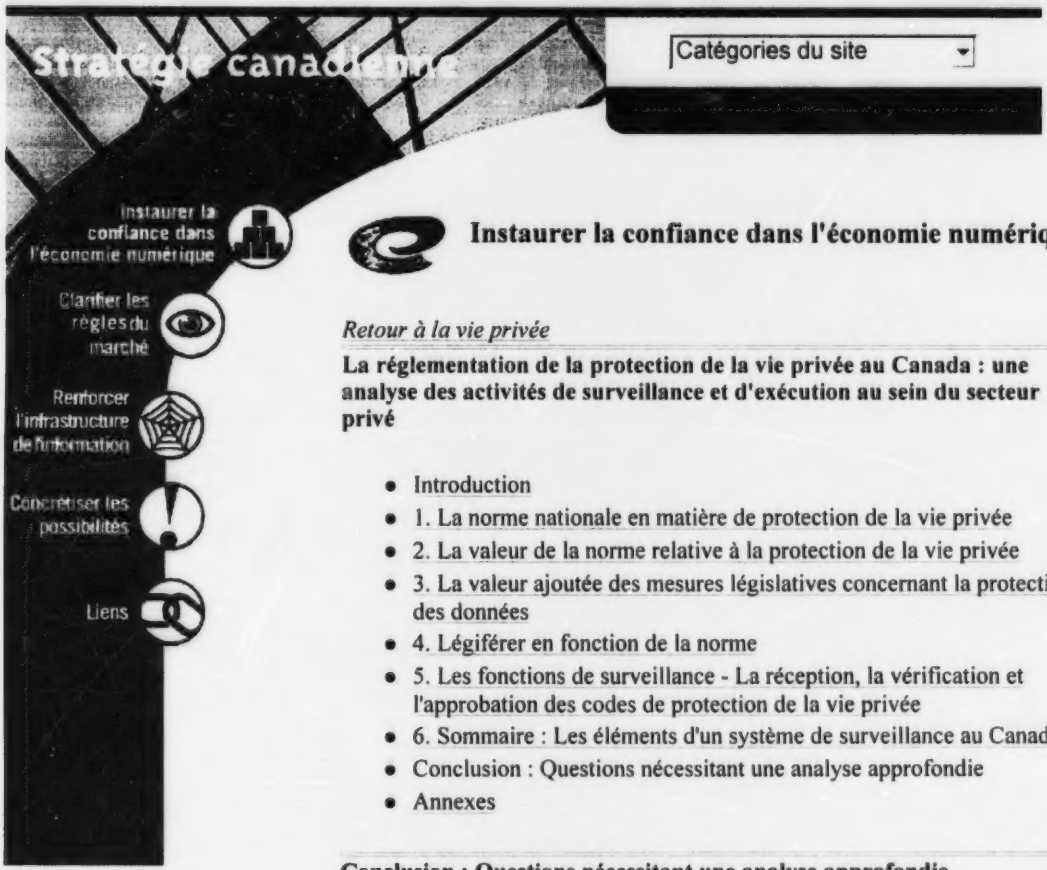
- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000



Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexes

Conclusion : Questions nécessitant une analyse approfondie

Les conclusions qui précèdent ne sont pas incompatibles avec d'autres analyses de principe récentes portant sur la protection des données. Elles sont cependant provisoires et incomplètes. Je conclus mon exposé par une liste de certaines des questions réglementaires complexes qui requièrent encore une analyse et des discussions approfondies.

Le Code type de la CSA est-il compatible avec les dispositions relatives à la protection de la vie privée qui sont actuellement en vigueur au Canada et à l'étranger?

S'il faut donner force de loi aux principes que comporte le Code type de la CSA, il est manifestement nécessaire d'analyser soigneusement le rapport qui existe entre le libellé de ces principes et celui des lois actuelles en matière de

protection de la vie privée, dont : la *Loi sur la protection des renseignements personnels* du gouvernement fédéral, les lois provinciales en matière d'accès à l'information et de protection de la vie privée, ainsi que le projet de loi 68 du Québec. En outre, il est nécessaire d'analyser la compatibilité de ce code avec d'autres dispositions relatives à la protection de la vie privée dans le secteur privé, dont celles qui figurent dans la *Loi sur les télécommunications* de 1993, la *Loi sur les banques* de 1991 et les lois provinciales en matière de crédit à la consommation. Il nous faut aussi comparer soigneusement le Code type de la CSA et la Directive de l'UE sur la protection des données.

Quel est le rapport futur entre les commissaires à la protection de la vie privée et d'autres organismes fédéraux et provinciaux de réglementation ?

Quel devrait être le rôle permanent des organismes fédéraux de réglementation comme le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) et le Bureau du surintendant des institutions financières (BSIF)? Le Conseil, en particulier, a été actif sur le plan de la réglementation de l'usage de nouvelles technologies au sein du secteur des télécommunications. D'aucuns font valoir qu'il ne faudrait pas diluer ce pouvoir de réglementation. À l'échelon provincial, quel serait le rôle que joueraient les organismes de réglementation du secteur de l'assurance et du crédit à la consommation?

Les commissaires à la protection de la vie privée devraient-ils être habilités à limiter les données personnelles transmises aux entreprises qui ne disposent pas de mesures convenables de protection des données?

L'un des soucis des instances européennes de protection des données est que les données personnelles peuvent être transmises par des sociétés disposant d'une protection « adéquate » à des sociétés qui n'en ont pas. Idéalement, chaque loi nationale sur la protection des données devrait contenir une restriction sur la circulation transfrontalière des données, similaire à celles que renferment les articles 25 et 26 de la Directive de l'UE. Dans ce cas, comment ce pouvoir devrait-il être exercé au Canada, et par qui? À quel stade les impulsions électroniques fugaces et rapides qui caractérisent la circulation internationale des données sont-elles visées par la réglementation canadienne?

Les mesures de surveillance de la conformité prises en vertu de la norme CSA seront-elles compatibles avec les régimes de surveillance que prévoit à l'heure actuelle la législation relative au secteur public?

Le Quality Management Institute de la CSA est en voie de se prononcer sur le système d'adhésion qui convient le mieux à la norme Q830. Si l'on recourt à l'adhésion à la norme en tant que processus de surveillance de la conformité, il sera nécessaire de disposer d'un guide de vérification cohérent, d'un système d'agrément des vérificateurs de la protection de la vie privée, d'un mécanisme de publicité convenable, d'une façon de vérifier les prétentions faites au sujet des politiques et des pratiques des entreprises et, peut-être, d'un symbole ou d'un sceau approprié pour les entreprises soucieuses de protéger la vie privée. Les commissaires à la protection de la vie privée doivent avoir confiance dans le processus d'adhésion si l'on veut que le Code type soit utilisé de la même façon que d'autres normes relatives à la gestion de la qualité.

Peut-on inclure dans une loi un pouvoir de réglementation pour exiger l'adhésion à une norme?

Il s'agit là d'une innovation intéressante et d'un moyen peut-être fort efficace de vérifier la conformité. Mais quels sont les précédents dans d'autres domaines, comme les achats de l'État, la politique en matière d'équité, la politique en matière d'environnement, etc.? S'il survient d'autres infractions dans une entreprise qui adhère à la norme, qui partage la responsabilité des dommages que peut avoir subi le sujet des données?

Quels sont les coûts d'un régime de surveillance, et par qui devrait-il être supportés? Existe-t-il des possibilités de recouvrement?

Un système de surveillance coordonné par les commissaires existants, systémique plutôt que spécifique, proactif plutôt que réactif, et éducatif plutôt que réglementaire, sera vraisemblablement aussi plus rentable. Le recours à un processus d'adhésion à une norme peut aussi libérer les commissaires et d'autres organismes de réglementation d'une grande partie du travail de vérification de la conformité et transmettre les frais encourus à l'utilisateur des données.

Quel processus convient-il d'utiliser pour la coordination fédérale-provinciale?

La question constitutionnelle fédérale-provinciale sous-tend toute cette analyse. Peu de choses sont possibles sans une entente de collaboration entre le gouvernement fédéral et les provinces au sujet d'un processus législatif approprié. Lawson a décrit six modèles, qui s'ajoutent au « modèle des normes nationales prépondérantes » : le modèle de la législation miroir, le modèle de l'abstention d'un niveau de compétence, le modèle contractuel, le modèle de la législation conditionnelle, le modèle de la législation parallèle, et le modèle de collaboration/complémentarité. Dans la mesure où il est possible de s'entendre sur le processus, cela facilitera le règlement de ces questions de surveillance et d'exécution.

En conclusion, il est possible de faire remarquer qu'il n'est pas nécessaire de tout conclure et fixer de manière définitive. La législation est un cadre; il faut qu'elle puisse s'adapter aux circonstances. Il faut aussi qu'elle soit accessible et conviviale. Plus les dispositions législatives sont compliquées, moins il y a de chances que les citoyens ordinaires s'en servent comme instrument. Il est possible toutefois qu'il ressorte de cette analyse une démarche distinctement canadienne en matière de protection des données personnelles, une démarche qui mette l'accent sur l'emploi de tous les instruments possibles que contient la « boîte à outils » de la protection de la vie privée. Elle reconnaît qu'une action volontaire menée du « bas vers le haut » est tout aussi nécessaire qu'une action réglementaire menée du « haut vers le bas ». Et elle comporte une combinaison innovatrice de la démarche classique du protecteur des citoyens et de l'utilisation des instruments relativement nouveaux du monde de l'élaboration des normes et de la certification.

- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000

Instaurer la confiance dans l'économie numérique

Retour à la vie privée

La réglementation de la protection de la vie privée au Canada : une analyse des activités de surveillance et d'exécution au sein du secteur privé

- Introduction
- 1. La norme nationale en matière de protection de la vie privée
- 2. La valeur de la norme relative à la protection de la vie privée
- 3. La valeur ajoutée des mesures législatives concernant la protection des données
- 4. Légiférer en fonction de la norme
- 5. Les fonctions de surveillance - La réception, la vérification et l'approbation des codes de protection de la vie privée
- 6. Sommaire : Les éléments d'un système de surveillance au Canada
- Conclusion : Questions nécessitant une analyse approfondie
- Annexes

ANNEXE 1

Pouvoirs accordés aux commissaires à l'information et à la protection de la vie privée en matière d'enquêtes sur les plaintes et de règlement de ces dernières.

Échelon fédéral

Le commissaire à la protection de la vie privée a le pouvoir de :

- sommer des personnes à comparaître devant lui et contraindre ces dernières à témoigner sous serment, de vive voix ou par écrit, ainsi que de produire les documents et choses qu'il juge nécessaires à l'enquête et à l'examen relatifs à la plainte, de la même façon et dans la même mesure qu'une cour supérieure d'archives;

- faire prêter serment;
- recevoir et admettre de telles preuves et d'autres informations, que ces preuves ou ces informations soient admissibles ou non devant une cour de justice;
- pénétrer dans toute installation qu'occupe une institution gouvernementale en respectant les exigences de cette dernière quant à la sécurité de l'installation en question;
- dans ladite installation, s'entretenir en privé avec toute personne et demander des informations dans les limites du pouvoir du Commissaire à la protection de la vie privée;
- examiner ou obtenir des copies ou des extraits de registres ou d'autres pièces trouvés dans ladite installation et contenant toute question pertinente à l'enquête.

Ontario

- Le commissaire peut obliger à produire et examiner tout document se trouvant sous la garde ou le contrôle d'une institution, indépendamment des dispositions des parties II et III de la Loi sur l'accès à l'information et la protection de la vie privée de 1987 et de tout autre loi ou privilège, et pénétrer dans toute installation qu'occupe une institution et l'inspecter en vue de l'enquête.
- Le dirigeant d'une institution peut exiger que le commissaire examine sur les lieux l'original d'un document qui l'intéresse.
- Le commissaire peut sommer à comparaître et interroger sous serment toute personne qui, à son avis, peut détenir des renseignements liés à l'enquête, et, à cette fin, il peut faire prêter serment à cette personne.

Colombie-Britannique

- Lorsqu'il procède à une enquête, le commissaire est investi des pouvoirs que lui accordent les articles 15 et 16 de la Inquiry Act.
- Le commissaire peut exiger que n'importe quel document lui soit produit et examiner tous les renseignements que contient ce dernier, y compris des informations personnelles.
- Indépendamment de tout autre texte de loi ou de tout privilège lié au droit de la preuve, un organisme public est tenu de produire au commissaire, dans un délai de dix jours, tout document ou copie d'un tel document qui est exigé.
- Lorsqu'un organisme public est tenu de produire un document et qu'il n'est pas possible d'en faire une copie, le dirigeant dudit organisme peut exiger que le commissaire examine l'original sur les lieux.

Alberta

- Lorsqu'il procède à une enquête, le commissaire est investi de tous les pouvoirs, privilèges et immunités que lui accorde la Public Inquiries Act.
- Le commissaire peut exiger que n'importe quel document lui soit produit, et examiner tous les renseignements que contient ce dernier, y compris les informations personnelles, que ledit document soit assujetti ou non aux dispositions de la Freedom of Information and Protection of Privacy Act.
- Indépendamment de tout autre texte de loi ou privilège lié au droit de

la preuve, un organisme public est tenu de produire au commissaire, dans un délai de dix jours, tout document ou copie d'un document qui est exigé.

- Lorsqu'un organisme public est tenu de produire un document et qu'il n'est pas possible d'en faire une copie, le dirigeant dudit organisme peut exiger que le commissaire examine l'original sur les lieux.

Québec (secteur public)

La commission peut étudier :

- un dossier confidentiel afin de déterminer si les renseignements nominatifs qu'il contient ont été consignés et utilisés d'une manière conforme à l'ordonnance; et si la confidentialité des renseignements personnels que contient un dossier détenu par un organisme public à propos de l'adoption d'une personne a été respectée;
- si la confidentialité des renseignements personnels que contient un dossier détenu par le Curateur public à propos d'une personne que ce dernier représente ou dont il administre les biens a été respectée;
- L'enquête est secrète. Seul un membre de la commission ou du personnel de direction de ce dernier, que la commission désigne à cette fin par écrit, peut examiner les renseignements nominatifs ou personnels figurant dans un dossier. Cependant, un membre du personnel de la commission peut, avec l'autorisation écrite de cette dernière, examiner les renseignements personnels que contient un dossier.

Québec (secteur privé)

Toute personne autorisée par la commission à procéder à une enquête peut :

- pénétrer, à toute heure raisonnable, dans les installations d'une entreprise exploitée par une personne qui recueille, tient, utilise ou communique à des tiers des renseignements personnels;
- examiner et faire des copies de tout renseignement personnel, sous quelque forme que ce soit;
- La commission peut faire enquête, ou charger une personne de le faire, au sujet de toute question concernant la protection de renseignements personnels, ainsi qu'au sujet des pratiques d'une personne qui exploite une entreprise et recueille, tient, utilise ou communique à des tiers de telles informations.

ANNEXE 2

Pouvoirs d'exécution des commissaires à l'information et à la protection de la vie privée.

Échelon fédéral

Le commissaire à la protection de la vie privée peut :

- demander à la Cour d'examiner tout refus de communiquer des renseignements personnels demandés au sujet desquels une enquête a été menée par le commissaire à la protection de la vie privée, à la

condition que ce dernier ait obtenu le consentement de la personne qui a demandé d'avoir accès auxdits renseignements;
- comparaître devant la Cour pour le compte de toute personne ayant demandé un contrôle judiciaire;
- avec l'autorisation de la Cour, comparaître à titre de partie à tout contrôle judiciaire demandé;
- Si elle détermine que le dirigeant de l'institution n'est pas autorisé par la Loi à refuser de communiquer les renseignements personnels en question, la Cour doit ordonner à cette personne de communiquer lesdites informations, sous réserve des conditions que la Cour estime appropriées, à la personne qui a demandé d'y avoir accès, ou rendre tout autre ordonnance que la Cour estime appropriée.

Ontario

- Après avoir reçu toutes les preuves nécessaires à une enquête, le commissaire peut se prononcer, par voie d'ordonnance, sur les questions soulevées par l'appel;
- Lorsque le commissaire confirme la décision du dirigeant d'un organisme selon laquelle celui-ci peut refuser de communiquer un document en tout ou en partie, il ne peut ordonner que le dirigeant communique le dossier en tout ou en partie;
- L'ordonnance du commissaire peut contenir toutes les conditions que ce dernier estime appropriées.

Colombie-Britannique

Si l'enquête se rapporte à la décision du dirigeant d'un organisme public de donner accès ou de refuser de donner accès à un dossier en tout ou en partie, le Commissaire doit, par voie d'ordonnance, prendre l'une des mesures suivantes :

- obliger le dirigeant à donner à la partie requérante accès au dossier en tout ou en partie, s'il décide que le dirigeant n'est pas autorisé à refuser cet accès ou tenu de le faire;
- confirmer la décision du dirigeant ou obliger ce dernier à réviser sa décision, s'il détermine que le dirigeant en question est autorisé à refuser l'accès;
- obliger le dirigeant à refuser l'accès à un dossier en tout ou en partie, s'il détermine que le dirigeant en question est tenu de refuser cet accès.

Si l'enquête porte sur toute autre question, le commissaire peut, par voie d'ordonnance, prendre une ou plusieurs des mesures suivantes :

- exiger d'exécuter une obligation imposée par la Loi ou le règlement connexe;
- confirmer ou réduire la prolongation d'un délai prévu à l'article 10 de la Loi;
- confirmer ou réduire des frais, ou ordonner un remboursement, dans les circonstances appropriées, y compris lorsqu'un délai n'est pas respecté;
- confirmer une décision de ne pas rectifier des renseignements personnels, ou préciser de quelle manière les rectifier;

- obliger un organisme public à cesser de recueillir, d'utiliser ou de communiquer des renseignements personnels d'une manière contraire à la Loi;
- obliger le dirigeant d'un organisme public à détruire les renseignements personnels qu'il a recueillis d'une manière contraire à la Loi.

Alberta

Si l'enquête se rapporte à une décision de donner accès ou de refuser de donner accès à un dossier en tout ou en partie, le commissaire peut, par voie d'ordonnance, prendre les mesures suivantes :

- obliger le dirigeant à donner à la partie requérante accès au dossier en tout ou en partie, s'il détermine que le dirigeant en question n'est pas autorisé à refuser cet accès ou tenu de le faire;
- confirmer la décision du dirigeant ou obliger ce dernier à la réviser, s'il détermine que le dirigeant est autorisé à refuser cet accès;
- obliger le dirigeant à refuser de donner accès au dossier en tout ou en partie, s'il détermine que le dirigeant est tenu de refuser cet accès.

Si l'enquête porte sur toute autre question, le Commissaire peut, par voie d'ordonnance, prendre une ou plusieurs des mesures suivantes :

- exiger qu'une obligation imposée par la Loi ou le règlement soit exécutée; confirmer ou réduire la prolongation d'un délai prévu à l'article 13 de la Loi;
- confirmer ou réduire des frais, ou ordonner un remboursement, dans les circonstances appropriées, y compris lorsqu'un délai n'est pas respecté;
- confirmer une décision de ne pas rectifier les renseignements personnels, ou préciser comment ces derniers doivent être rectifiés;
- obliger un organisme public à cesser de recueillir, d'utiliser ou de communiquer des renseignements personnels d'une manière contraire à la Loi;
- obliger le dirigeant d'un organisme public à détruire les renseignements personnels qu'il a recueillis d'une manière contraire à la Loi.

Québec (secteur public)

La Commission peut, après avoir fait enquête sur un dossier contenant des renseignements personnels ou un dossier confidentiel, et après avoir donné à l'organisme public chargé dudit dossier l'occasion de présenter des observations écrites :

- ordonner que les renseignements nominatifs en question soient corrigés ou supprimés du dossier, ou que l'utilisation du dossier soit rendue contraire à la Loi, l'ordonnance ou les prescriptions de la Commission, selon le cas, peuvent être suspendues;
- ordonner à l'organisme public de prendre les mesures qu'il estime appropriées pour remplir les conditions prévues par la Loi ou les prescriptions de la Commission;
- ordonner la destruction d'un dossier contenant des renseignements

personnels qui a été établi ou est utilisé d'une manière contraire à la Loi;
- recommander au gouvernement de modifier ou révoquer l'ordonnance autorisant l'établissement d'un dossier confidentiel.

À la conclusion d'une enquête, la Commission peut :

- ordonner à l'organisme public de prendre les mesures qui s'imposent pour garantir la confidentialité des renseignements personnels que contient un dossier relatif à l'adoption d'une personne;
- indiquer les mesures qui doivent être prises pour garantir la confidentialité des renseignements personnels que contient un tel dossier;
- indiquer les conditions spéciales auxquelles peut être soumise la tenue d'un tel dossier.

Québec (secteur privé)

- La Commission est investie de tous les pouvoirs nécessaires pour exercer sa compétence; il lui est possible de rendre toute ordonnance qu'elle juge appropriée afin de protéger les droits des parties, et de se prononcer sur toute question de fait ou de droit;
- La Commission peut ordonner à une personne qui exploite une entreprise de communiquer ou corriger des renseignements personnels ou d'éviter de le faire;
- Une décision de la Commission devient exécutoire comme s'il s'agissait d'un jugement de la Cour supérieure, et elle a tous les effets d'un tel jugement à compter de la date de son homologation par la Cour supérieure;
- À la suite d'une enquête sur la collecte, la tenue ou la communication de renseignements personnels par une personne qui exploite une entreprise, la Commission peut, après avoir donné à cette personne la possibilité de présenter ses observations, recommander ou ordonner la prise de mesures correctives jugées appropriées pour garantir la protection des renseignements personnels.

ANNEXE 3

Fonctions consultatives des commissaires ou commissions à l'information et à la protection de la vie privée au sujet des répercussions de dispositions législatives et de technologies sur la protection de la vie privée.

Échelon fédéral

- Le commissaire à la protection de la vie privée peut, à toute époque de l'année, présenter au Parlement un rapport spécial sur toute question relevant de ses pouvoirs et fonctions.

Ontario

- Le commissaire peut formuler des commentaires au sujet des répercussions de projets de régime législatif ou de programme gouvernemental sur la protection de la vie privée.

Colombie-Britannique

Le Commissaire peut :

- formuler des commentaires au sujet des répercussions de projets de régime législatif ou de programme d'organismes publics sur l'accès à l'information ou la protection de la vie privée;
- formuler des commentaires au sujet des répercussions de systèmes automatisés de collecte, de stockage, d'analyse ou de transferts de renseignements sur l'accès à l'information ou la protection de la vie privée;
- formuler des commentaires au sujet des répercussions, sur la protection de la vie privée, de l'utilisation ou de la communication de renseignements personnels pour fins de couplage de dossiers.

Alberta

Le Commissaire peut :

- formuler des commentaires au sujet des répercussions de projets de régime législatif ou de programme d'organismes publics sur l'accès à l'information ou la protection de la vie privée;
- formuler des commentaires au sujet des répercussions, sur la protection de la vie privée, de l'utilisation ou de la communication de renseignements personnels pour fin de couplage;
- donner des conseils et formuler des recommandations de nature générale au dirigeant d'un organisme public au sujet de questions relatives aux droits ou aux obligations de ce dirigeant aux termes de la Loi.

Québec (secteur public)

Le rapport annuel de la Commission peut contenir :

- des recommandations destinées à promouvoir la protection des renseignements personnels, ainsi que l'exercice du droit de consulter des documents, notamment de la part de personnes handicapées et de membres des communautés culturelles;
- des propositions liées aux normes techniques de préservation, de classification, d'extraction de documents, ainsi qu'aux méthodes de consultation de ces derniers.

Québec (secteur privé)

- La Commission doit, le 1er octobre 1997 au plus tard, et aux cinq ans par la suite, présenter au gouvernement un rapport sur l'application de la Loi.

ANNEXE 4

Fonctions d'éducation publique et de recherche des commissaires à l'information et à la protection de la vie privée.

Échelon fédéral

- Le commissaire à la protection de la vie privée doit, dans les trois mois qui suivent la fin de chaque exercice, présenter au Parlement un rapport annuel sur les activités du bureau durant l'exercice en question;
- Le commissaire à la protection de la vie privée doit, en tout temps, présenter au Parlement un rapport spécial sur toute question relevant des pouvoirs et des fonctions du Commissaire.

Ontario

- Le commissaire est tenu de présenter un rapport annuel au président de l'Assemblée législative. Ce rapport doit comprendre un examen exhaustif de l'efficacité de la Loi et de la Loi sur l'accès à l'information municipale et la protection de la vie privée de 1989, pour ce qui est de donner accès à l'information et de protéger la vie privée;

Le commissaire peut :

- entreprendre ou commander des recherches sur des questions qui ont une incidence sur la réalisation des objectifs de la Loi;
- exécuter des programmes d'éducation publique et fournir des renseignements au sujet de la Loi et du rôle et des activités du commissaire;
- recevoir du public des commentaires sur l'application de la Loi.

Colombie-Britannique

- Le commissaire doit rendre compte chaque année au président de l'Assemblée législative des activités de son bureau, ainsi que de toute plainte ou de tout examen découlant d'une décision, d'une mesure ou du défaut de prendre une mesure de la part du commissaire à titre de dirigeant d'un organisme public;

Le commissaire peut :

- renseigner le public sur la Loi;
- recevoir des commentaires du public sur l'application de la Loi;
- entreprendre ou commander des recherches sur toute question ayant une incidence sur la réalisation des objectifs de la Loi.

Alberta

- Le commissaire est tenu de rendre compte chaque année au président de l'Assemblée législative des activités de son bureau, de toute plainte ou tout examen découlant d'une décision, d'une mesure ou du défaut de prendre une mesure de la part du commissaire à titre de dirigeant d'un organisme public, ainsi que de toute autre question concernant l'accès à l'information et la protection de la vie privée, selon ce qu'il juge approprié;

Le commissaire peut :

- lancer une enquête pour s'assurer que l'on se conforme à toute disposition de la Loi ou aux règles relatives à la destruction des dossiers qui sont énoncées dans tout autre texte de loi de l'Alberta, ou un règlement ou un autre instrument juridique en vertu duquel agit un organisme public local;
- renseigner le public sur la Loi;
- recevoir les commentaires du public sur l'application de la Loi;
- entreprendre ou commander des recherches sur toute question ayant une incidence sur la réalisation des objectifs de la Loi.

Québec (secteur public)

- La Commission doit envoyer au ministre désigné, avant le 30 juin de chaque année au plus tard, un rapport sur ses activités au cours de l'exercice précédent. Le rapport doit porter sur la façon dont la Loi est observée, et les moyens dont dispose la Commission pour l'appliquer;

Le rapport peut aussi contenir :

- des recommandations destinées à promouvoir la protection des renseignements personnels, et l'exercice du droit de consulter des documents, notamment par les personnes handicapées et les membres des communautés culturelles;
- des propositions liées aux normes techniques de préservation, de classification et d'extraction de documents, ainsi qu'à la méthode de consultation de ces derniers;
- des suggestions du public sur toute question relevant de la compétence de la Commission.

Québec (secteur privé)

- La Commission doit, au plus tard le 1er octobre 1997, et aux cinq ans par la suite, présenter au gouvernement un rapport sur l'application de la Loi;
- Dans l'année qui suit le dépôt d'un rapport auprès de l'Assemblée nationale, un comité désigné doit examiner s'il est souhaitable de préserver la Loi telle qu'elle se présente ou de la modifier, et entendre aussi les observations des personnes et des organisations intéressées sur de telles questions.

ANNEXE 5

Mandats des commissaires à l'information et à la protection de la vie privée.

Échelon fédéral

- Le commissaire à la protection de la vie privée occupe sa charge à titre inamovible pendant une période de sept ans, mais peut être démis de ses fonctions à quelque moment que ce soit par le gouverneur en conseil, à la demande du Sénat et de la Chambre des communes.

Ontario

- Le commissaire occupe sa charge pendant cinq ans et peut être nommé de nouveau pendant une ou plusieurs périodes supplémentaires; il peut toutefois être démis de ses fonctions pour motif valable par le lieutenant-gouverneur en conseil, à la demande de l'Assemblée.

Colombie-Britannique

- Le commissaire occupe sa charge pendant six ans, et n'a pas le droit d'être nommé de nouveau à ce poste.

Alberta

- Le commissaire occupe sa charge pendant cinq ans;
- La personne qui occupe la charge de commissaire continue de le faire après l'expiration de son mandat jusqu'à ce qu'elle soit nommée de nouveau, qu'un successeur soit nommé ou qu'il se soit écoulé une période de six mois, suivant la première de ces trois éventualités.

Québec (secteur public)

- Le mandat des membres de la Commission ne peut excéder cinq ans;
- Les membres de la Commission ne peuvent en aucun cas être nommés pour plus de deux mandats consécutifs.

Québec (secteur privé)

- La Commission d'accès à l'information est créée par la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

- Instaurer la confiance dans l'économie
- Sécurité et cryptographie
- Protection des consommateurs

Page d'accueil du Groupe de travail

Aide Quoi de neuf Carte du site Opinion Contexte English Haut de la page

Canada

Révisé le 10/04/2000